NATIONAL ARCHIVES

Inspector General

December 22, 2021

TO: David S. Ferriero
Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General

SUBJECT: *National Archives and Records Administration's Fiscal Year 2021 Federal Information Security Modernization Act of 2014 Audit*
OIG Report No. 22-AUD-04

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 2021.

CLA is responsible for the attached auditor's report dated December 21, 2021 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 were increased maturation of Risk Management, Identity and Access Management, and Information Security Continuous Monitoring from the "Ad Hoc" level to "Defined." In addition, three additional domains were assessed at the "Defined" level (Security Training, 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 24 new recommendations to help NARA address challenges in its development of a mature and effective information security program. In addition, CLA noted all 24 recommendations related to prior FISMA audits are still open.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this letter. As with all OIG products, we determine what information is publicly posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended,* we will provide copies of our report to congressional committees with oversight responsibility over NARA.

We appreciate the cooperation and assistance NARA extended to CLA and my staff during the audit. Please contact me or Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachment

cc: Debra Wall, Deputy Archivist of the United States
Micah Cheatham, Chief of Management and Administration
William Bosanko, Chief Operating Officer
Swarnali Haldar, Chief Information Officer
Gary M. Stern, General Counsel
Meg Ryan Guthorn, Acting Deputy Chief Operating Officer
Kimm Richards, Accountability
Jewel Butler, Assistant Inspector General for Audits
Kimberly Boykin, Audit Director
Carol Seubert, Senior Financial Auditor
Andrew Clements, Senior IT Auditor
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

National Archives and Records Administration's 2021 Federal Information Security Modernization Act of 2014 Audit

Final Report

December 21, 2021

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

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

December 21, 2021

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

Dear Mr. Baker:

CliftonLarsonAllen LLP (CLA) is pleased to present our performance audit report 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 2021.

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) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or Act) for fiscal year (FY) 2021. FISMA requires agencies to develop, implement, and document an agency-wide information security program and practices. The Act also requires Inspectors General (IG) 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 the FISMA and applicable instructions from the OMB and Department of Homeland Security (DHS) IG FISMA Reporting Metrics.

For FY 2021, OMB required IGs to assess 66 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 (GAGAS). 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 OMB's FY 2021 FISMA reporting metrics, we reviewed select controls for a sample of 10 NARA FISMA reportable systems, interviewed agency officials, and reviewed information, including system security documentation. Refer to Appendix A for background on the FISMA legislation and Appendix B for details on our scope and methodology. We also reviewed the status of the 24 open FISMA prior year recommendations related to NARA's security program and practices. Appendix C contains the current year status of prior FISMA report recommendations. Appendix D provides a listing of the representative subset of sampled systems. Appendix E provides a listing of acronyms used throughout this report.

Based upon our audit of NARA's information security program, including its compliance with FISMA and OMB/DHS requirements in the function areas, we 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 were increased maturation of Risk Management, Identity and Access Management, and Information Security Continuous Monitoring from the "Ad Hoc" level to "Defined." In addition, three additional domains were assessed at the "Defined" level (Security Training, Incident Response, and Contingency Planning) and three domains at the "Ad Hoc" level (Supply Chain Risk Management, Configuration Management, and Data Protection and Privacy). 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.

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

We made 24 new recommendations to help NARA address challenges in its development of a mature and effective information security program. In addition, we noted all 24 recommendations related to prior FISMA audits are still open.

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 included in this report was obtained from NARA on or before December 21, 2021. We have no obligation to update our report or to revise the information contained herein to reflect events occurring subsequent to December 21, 2021.

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

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

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Arlington, Virginia
December 21, 2021

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 (IG) 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 audit was to assess the effectiveness of NARA's information security program in accordance with the FISMA of 2014 and applicable instructions from OMB and the Department of Homeland Security (DHS) IG FISMA Reporting Metrics (the metrics).[2]

To address OMB's FY 2021 FISMA reporting metrics, we reviewed select controls for a sample of 10 NARA FISMA reportable systems, interviewed agency officials, and reviewed information, including system security documentation. Refer to Appendix A for background on the FISMA legislation and Appendix B for details on our scope and methodology. We also reviewed the status of the 24 open FISMA prior year recommendations related to NARA's security program and practices. Appendix C contains the current year status of prior FISMA report recommendations. Appendix D provides a listing of the representative subset of sampled systems. Appendix E provides a listing of acronyms used throughout this report. Appendix F provides agency comments.

Based upon our audit of NARA's information security program, including its compliance with FISMA and OMB/DHS requirements in the function areas, we 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 were increased maturation of Risk Management, Identity and Access Management, and Information Security Continuous Monitoring from "Ad Hoc" level to "Defined." In addition, three additional domains were assessed at the "Defined" level (Security Training, Incident Response, and Contingency Planning) and three domains at the "Ad Hoc" level (Supply Chain Risk Management, Configuration Management, and Data Protection and Privacy). 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.

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

[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 2021 IG FISMA Reporting Metrics to NARA OIG as a separate deliverable under the contract for this performance audit.

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

We made 24 new recommendations to help NARA address challenges in its development of a mature and effective information security program.[3] In addition, we noted all 24 recommendations related to prior FISMA audits are still open.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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, including its compliance with FISMA and OMB/DHS requirements in the function areas, we concluded that NARA's information security program was "Not Effective." While NARA's overall maturity level has not changed from last year, notable this year were increased maturation of Risk Management, Identity and Access Management, and Information Security Continuous Monitoring from the "Ad Hoc" level to "Defined." In addition, three additional domains were assessed at the "Defined" level (Security Training, Incident Response, and Contingency Planning) and three domains at the "Ad Hoc" level (Supply Chain Risk Management, Configuration Management, and Data Protection and Privacy) as shown in **Table 1** below.

Table 1: FY 2021 IG Cybersecurity Framework Function and Domain Ratings

Cybersecurity Framework Security Functions[4]	FY 2021 Maturity Level by Function	Metric Domains	Domain Maturity Level	Change from FY 2020
Identify	Defined (Level 2)	**Risk Management**	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
		Supply Chain Risk Management[5]	Ad Hoc (Level 1)	Not Applicable
Protect	Defined (Level 2)	**Configuration Management**	Ad Hoc (Level 1)	No Change

[3] Several of these new recommendations were reported as recommendations within the FY2021 NARA Financial Statement audit report and are also being repeated within this report since they also directly relate to FISMA audit findings being reported. Additionally, the financial statement audit scope is focused upon financially significant information systems, compared to the FISMA audit which applies to all NARA systems.

[4] 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.

[5] This domain will not be considered in the Identify framework function rating for FY 2021.

Cybersecurity Framework Security Functions[4]	FY 2021 Maturity Level by Function	Metric Domains	Domain Maturity Level	Change from FY 2020
		Identity and Access Management	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
		Data Protection and Privacy	Ad Hoc (Level 1)	No Change
		Security Training	Defined (Level 2)	No Change
Detect	Defined (Level 2)	**Information Security Continuous Monitoring**	Defined (Level 2)	Upgraded from Ad Hoc (Level 1)
Respond	Defined (Level 2)	**Incident Response**	Defined (Level 2)	No Change
Recover	Defined (Level 2)	**Contingency Planning**	Defined (Level 2)	No Change
Overall	**Not Effective**			**No Change**

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.

- Enhancements were made to NARA *Cyber Security Framework Methodology Processes & Procedures*, v1.15 (12/15/2020) (CFM) to reduce inconsistencies previously noted when compared to other methodologies, policies and procedures and existing practices and controls.
- NARA has significantly strengthened its completion rate for annual security awareness training.
- Improvements were made to NARA's security assessment and authorization documentation such as updates to system security plans and security control assessments.
- NARA has strengthened its assignment of Information System Security Officers (ISSO) to FISMA reportable systems, with corresponding improvements in the development and update of security assessment and authorization documentation.

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 process better adapts to risk level impacted changes.
- Information security weaknesses are more consistently documented, monitored, and closed.
- Multi factor authentication is implemented agency-wide.
- User account management processes related to documentation, account reviews, account monitoring and the separation process are strengthened.
- Privacy specific training requirements for individuals with responsibility for Personally Identifiable Information (PII) is implemented.
- Configuration management plans, policies and procedures are either developed or enhanced.
- 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.

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 a lack of 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 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:

- Policy Development
  - Inconsistencies were found within the CFM or between the CFM and other policy and procedure documents, specifically, who is responsible to approve the closure of plans of actions and milestones.
  - Outdated personnel security and privacy policies and procedures were noted, which did not reflect current security controls and practices in place.
  - Comprehensive strategies and plans were not developed to address supply chain risk management (SCRM) or identity, credential and access management (ICAM) programs.

- Implementation of Policies and Procedures
  - When a change in Authorizing Official occurred, NARA did not document the new Authorizing Official acknowledgment of the risks to current systems.
  - Role-based privacy training has not been fully developed and deployed.
  - Contingency plans were inconsistently tested, due to conflicting requirements within the CFM and other policy and procedure documents.
  - User account reviews were not completed for all sampled systems.

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 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 years' reported weaknesses,[6] with 24 recommendations remaining unimplemented, we made 24 new recommendations to help NARA address challenges in its development of a mature and effective information security program.

Table 2: Weaknesses Noted in FY 2021 FISMA Audit Mapped to Domains in the FY 2021 IG FISMA Reporting Metrics

FY 2021 IG FISMA Metrics Domains	Weaknesses Noted
Risk Management	Plan of Action and Milestones (POA&Ms) and information security weaknesses were not effectively managed.
	Security Assessment and Authorization (SA&A) documentation was not reviewed when there was a change in Authorizing Official (AO), controls were not tested, or security documentation was incomplete.
	System hardware inventories were incomplete or not properly managed.
Supply Chain Risk Management	A supply chain risk management strategy or plan has not been developed.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Configuration management plans and policies were not consistently maintained.
Identity and Access Management	Incomplete deployment of two-factor user authentication mechanisms.
	Evidence of completed rules of behavior were missing in support of system access.
	Identity Control and Access Management policy and strategies were not developed.
	Personnel security policies and procedures were outdated.
	Inactive user accounts and those belonging to separated employees were not being disabled timely.
Data Protection and Privacy	NARA's privacy policy and procedures were out of date and targeted role-based privacy training was not provided to all personnel having responsibility for PII or for activities that involve PII.
Security Training	Security training requirements were not fully implemented.

[6] FY 2016 "Audit of NARA's Compliance with FISMA," OIG Report Number 16-02 (1/12/16) and FY2018 "Audit of National Archives and Records Administration's Compliance with the Federal Information Security Modernization Act," OIG Report Number 19-AUD-02 (12/21/18).

FY 2021 IG FISMA Metrics Domains	Weaknesses Noted
Information Security Continuous Monitoring	The annual continuous monitoring of information security controls was not performed consistently for all systems.
Contingency Planning	NARA did not perform contingency plan testing commensurate with the availability risk level of the information system.

The following section provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions.

- 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 the representative subset of sampled systems.
- Appendix E provides a listing of acronyms utilized throughout this report.
- Appendix F provides agency comments.
- Appendix G 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 addresses both security and privacy controls. NARA's information security risk management process focused on identifying and evaluating the threats and vulnerabilities to 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 gaps 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 effectively managed security weaknesses to ensure failed controls identified during security control assessments are formally tracked within POA&Ms, milestone completion dates are updated, closed weaknesses are properly supported and approved, and NARA has inconsistent requirements in terms of the POA&M closure process. NARA has also not ensured that security control assessments were conducted annually for all FISMA reportable systems. In addition, when a change in Authorizing Official occurred, NARA did not document the new Authorizing Official's acknowledgment of the risks to current systems even though NARA's Security Methodology for Certification & Accreditation and Security Assessment requires it.

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

POA&Ms

OMB Memorandum M-02-01*, Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for agency POA&Ms, to include deficiency descriptions, remediation actions, required resources, and responsible parties. In addition, POA&Ms identify what actions must be taken to remediate system security risks and improve NARA's overall information security posture.

POA&Ms were not effectively managed throughout NARA. Specifically, approvals were not always documented, POA&M milestone dates were not updated in a timely manner, POA&Ms were not always complete, and there were inadequate descriptions of the process to retain documentation in support of closed POA&Ms. The establishment, tracking, and remediation of information security weaknesses through the POA&M process is a significant process as part of the continuous monitoring of control weaknesses.

We noted the following regarding the creation of POA&Ms for failed system controls, and inadequate/missing evidence and approvals in support of closed POA&Ms.

- For 5 of 10 sampled systems, POA&Ms were missing attributes or had milestone dates which had passed. (AERIC, AERIC Title 13, ENOS/HMS, NARANET, and WTC)[7]
- For 6 of 10 sampled systems, controls indicated as "failed" during the most recent Security Assessment Report (SAR) did not result in either the creation of a POA&M, or POA&Ms were not created within the 10 business days of weakness discovery. (A2 PACS, AERIC, ENOS/HMS, NARANet, RCBS, and SCTS)
- The NARA CFM requires the Chief Information Security Officer (CISO) to approve closure of POA&Ms; however, the NARA ISSO Guide (version 1.8) requires only the ISSO to approve closure.[8] Additionally, there are contradictory procedures/statements indicated within the same procedure document. For example, within the *NARA IT Security Methodology for CA and Security Assessments* (version 7.5), under CA-5, when discussing the POA&M closure process, one bullet states "The Information System Security Manager (ISSM) will review the evidence of remediation for completeness and appropriateness. If the evidence of remediation appears to address the weakness the ISSM will submit to the CISO for final review and closure." However, 2 bullets down, it states "After the ISSM validates the POA&M as completed it can be marked as closed by the ISSO."
- For 23 of 25 sampled closed POA&Ms, insufficient documentation was provided in support of closure, and/or evidence of appropriate approval was missing. (AERIC, NARANet, OFAS, and SCTS)

Due to inconsistent policies and procedures related to POA&M management, approvals were not properly documented, and there were inadequate descriptions of the process to retain documentation in support of closed POA&Ms. In addition, for controls indicated within SARs which did not result in a POA&M, either NARA noted they were covered in a POA&M listing which was not provided, or POA&Ms were not created in a timely manner due to inadequate ISSO oversight.

Without properly managing POA&Ms, NARA is at risk of operating systems and applications with known security weaknesses that are not being adequately tracked or remediated. Further, without sufficient documentation to justify closure of POA&Ms, NARA cannot ensure that corresponding security risks have been fully mitigated.

Security Assessment and Authorization (SA&A)

NARA policy[9] 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[10] states that in the event of a change in authorizing officials, the new authorizing official should review the current authorization decision document, authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then they would sign a new authorization decision document. This process would formally transfer responsibility and accountability for the

[7] These represent systems in scope which described weaknesses were identified. Refer to Appendix D for a description of system acronyms.

[8] Although NARA provided a revised Cyber Security Framework Methodology: Processes and Procedures which removes references to the CISO in the POA&M closure process, as this revision was made on 9/1/2021, the noted inconsistency in policies and procedures was in place during most of FY 2021, and for the purposes of this audit, it was not relied upon by the auditors.

[9] NARA Cyber Security Framework Methodology Processes & Procedures, v1.15, 12/15/2020.

[10] NARA IT Security Methodology for Certification and Accreditation and Security Assessment, 5/20/202019, version 7.5.

information system or the common controls inherited by organizational information systems and explicitly accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation.

SA&A documentation was not effectively managed throughout NARA. 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 weaknesses related to the creation, maintenance, monitoring, and retention of SA&A documentation.

We noted the following weaknesses related to SA&A processes.

- For 7 of 10 sampled systems, although the AO listed within the Authorization to Operate (ATO), has subsequently changed from the former Chief Information Office (CIO)/Assistant Archivist for Information Services, a new authorization decision document has not been signed to indicate the new authorizing official (new CIO) is willing to accept the documented risk. (AERIC Title 13, AERIC, NARANET, OFAS, ENOS/HMS, RCPBS and SCTS) For 5 of 10 sampled systems, system security plans (SSPs) did not indicate completion or approval dates, so it was unclear when these documents were last reviewed or approved by the AO, the AO's designated representative, or the ISSO. Per the ISSO Guide "Appendix A," NARA ISSO Task List, ISSOs are to review, update (as needed) the SSP. NARA assumed the date printed in the footer each time the system security plan is printed was sufficient to indicate date completed, if not specifically indicated. Also, NARA indicated that the date of the last ATO represents the date each system security plan was approved. (NARANet, ECRM, OFAS, SCTS and WTC)
- An annual security control assessment was not performed for a system. Specifically, NARA completed nine out of ten sampled annual security control assessments. An annual assessment was not performed for one stand-alone, air-gapped system that resides in a SCIF NARA was unable to perform this assessment because it required physical access to the system in order to assess. Building closures and occupancy restrictions in response to the COVID-19 pandemic prevented physical access to the system to perform assessment activities. (AERIC Title 13)

These weaknesses were attributed to a lack of clarity within NARA's CFM related to Ongoing Authorizations and what constitutes a "change in status" for re-certification, and a lack of ISSO oversight. As a result, system re-certification efforts were not being performed upon a change an Authorizing Official.

Without documented evidence that the current authorizing official explicitly accepts the risks of the 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 annual security control assessments 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[11] 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 and is at the level of granularity deemed necessary for tracking and reporting.

However, NARA's asset management practices and controls, specific to the maintenance of hardware assets were determined to be inaccurate or inconsistently implemented. Weaknesses were noted in the content and taxonomy of hardware inventory listings and collection of NARA equipment upon employment separation.

Although NARA's 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 FY.

For 6 of 10 sampled systems, we noted that hardware asset inventories were not complete and were missing attributes identified such as Media Access Control (MAC) addresses or locations of assets. (A2 PACS, AERIC, AERIC Title 13, OFAS, WTC and ENOS/HMS) Upon bringing to management's attention, updated inventory listings for AERIC, AERIC Title 13, OFAS, A2 PACS and WTC were provided which included locations. In addition, the CFM was revised on 9/1/2021 to reflect a removal of the requirement for MAC addresses within hardware inventories. However, despite these updates, the noted discrepancies were still in place for a majority of FY 2021. 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 the following:

- NARA has not completed a laptop inventory 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 that a physical inventory is in process; however, this effort is not expected to be completed until December 2021.

- For 28 of 121 individuals who separated NARA employment between 10/1/2020 and 6/30/2021, these individuals were noted within NARA property management records as still assigned laptops with their status indicated as "In Service" per NARA's Asset Management Report (August 2021). However, per NARA Asset Management Standard Operating Procedures, the status of equipment reclaimed upon employment separation is to be changed to "In Inventory" within the Asset Management system.

- For one of the 28 separated individuals, they were assigned a total of 21 laptops. This individual was determined to be a site technician, who had not formally identified the specific individuals this equipment had been assigned to.

[11] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015 – security control, CM-8 Information System Component Inventory.

Due to the lack of a recent annual physical inventory to validate the accuracy of asset management inventory records, accompanied by the inaccurate reporting of equipment status and assignments, the content of these inventories was not accurate.

By not following standard data elements/taxonomy required by the agency for asset inventory content, there is an increased risk that assets may not be adequately tracked and reported, and potentially not adequately secured and protected. Also, without an accurate tracking of hardware assets and collecting this equipment upon an individuals' separation of employment, there is an increased risk of the misappropriation of assets.

Recommendations:
We recommend that the NARA CIO take the following actions, which include the prior unimplemented recommendations related to the weaknesses noted for the Risk Management domain:

1. Ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated timely; and are updated to include detailed information on the status of corrective actions. (Recommendation #6, FY 2018 FISMA Audit Report #19-AUD-02)

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. (New Recommendation)

3. Ensure plans of actions and milestones for the NARANet and OFAS systems are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives, to include enhanced POA&M closure procedures. (Recommendation #6, FY 2020 Financial Audit Report #21-AUD-03)

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. (New Recommendation)

5. Identify all FISMA reportable systems in which the Authorizing Official (AO) listed within the Authorization to Operate (ATO), has subsequently changed. (New Recommendation)

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 regards to requirements upon changes in AO. This is a separate activity from the ongoing authorization process. (New Recommendation)

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. (New Recommendation)

8. Identify all system security plans, which are missing attributes, then update so these values are populated. (New Recommendation)

9. Conduct a security control assessment of the AERIC Title 13 system, with results documented within a SAR. (New 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. (New Recommendation)

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. (New Recommendation)

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. (New Recommendation)

13. Reconcile departure reports received from Human Capital to the asset management inventory system, on a regular basis (e.g. monthly, quarterly, etc.) to ensure updates are being made in a timely manner and are accurate to reflect separated or transferred employees and contractors. (New Recommendation)

Metric Domain – Supply Chain Risk Management

FISMA requires each federal agency to develop, document and implement agency-wide strategies, policies and 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.

NARA has not developed and communicated an organization wide SCRM strategy and implementation plan to manage supply chain risks. In addition, current policies and procedures are not well defined. As an example, the NARA CFM primarily refers to supply chain risk management controls as being defined and documented within individual system security plans, however upon our review of sampled system security plans, references to even the term "supply chain," were minimal or non-existent.

This occurred because NARA management did not make it a priority to implement a SCRM strategy and implementation plan and fully develop policies and procedures. In addition, management is still awaiting further implementation directions from OMB and DHS to outline the process to address supply chain risk management strategy/action plans and related policy and procedural requirements of the SECURE Technology Act.[12]

Without the development of an SCRM strategy and implementation plan, NARA is at risk of inadequate continuous monitoring of their supply chain and the potential for disruption and impact to mission success in terms of malicious adversarial activity, espionage and data exfiltration.

[12] Public Law 115 - 390 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act' or the "SECURE Technology Act," 12/31/2021.

Recommendations:
We recommend that the NARA CIO take the following actions noted for the Supply Chain Risk Management domain:

14. Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks. (New Recommendation)

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 2021, weaknesses in the NARA IT environment continue to contribute to deficiencies in system configuration, data protection and privacy, access controls, and security training.

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

Metric Domain – Configuration Management

NARA continues to lack complete and consistent documentation and communication 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 4, security control SI-2, states that organizations are to install security-relevant software and firmware updates [within organization-defined time period] of the release of the updates, and per RA-5, the organization remediates legitimate vulnerabilities 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 2020 and before. Due to the vulnerabilities identified, the assessment team was able to exploit certain vulnerabilities. NARA's processes were not effective in tracking and remediating configuration vulnerabilities in network devices identified during internal vulnerability scans. In addition, management did not ensure devices deployed within the NARA network were hardened to prevent default or weak authentication mechanisms.

Management 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 indicated that due to requests for funding, which were not approved, this has impacted their ability to complete needed efforts related to its remediation of unsupported software.

An attacker may exploit the vulnerabilities identified to take control over certain systems, cause a denial-of-service attack, or gain unauthorized access to critical files and data. In addition, the inconsistent application of vendor patches could jeopardize the data integrity and confidentiality of NARA's sensitive information. Without remediating all significant security vulnerabilities, systems could be compromised, resulting in potential harm to data confidentiality, integrity, and availability.

Configuration Management Plans, Policies and Procedures

NIST SP 800-53, revision 4 requires that organizations develop, document, and disseminate a configuration management policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance. In addition, and procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Although NARA has developed configuration management plans and methodologies (such as the *Configuration Management Plan* (CMP) for NARA Information Technology Telecommunication Support Services (NITTSS O&M), CFM, and the NARA IT Security Methodology for Configuration Management), these documents were determined not comprehensive or complete. Specifically:

- NARA has not developed and communicated organization wide configuration management policies and procedures.

  Although NARA has indicated the CFM represents NARA's organization wide configuration management policies and procedures, We noted this document only describes Information Services Enterprise Change Advisory Board (ECAB) process to manage NARANet and systems managed by Information Services but not every NARA system. NARA utilizes Change Control Boards (CCB) in addition to the ECAB, which act as the change authority for the approval of change requests.

  NARA relies upon the CMP for NITTSS to apply to all NARA projects, to supplement the CFM. However, this CMP does not indicate it is applicable to all configuration items for all NARA systems, only those changes which affect NARANet.

- A formalized procedure has not been developed to manage and approve deviations from baseline system configurations which are not under ECAB control; however, some systems utilize a separate CCB.

- A CMP was not developed for a system (Websites to the Cloud (WTC)), in accordance with the NARA IT Security Methodology for Configuration Management.

These weaknesses were attributed to a combination of the following factors; NARA has not made it a priority to develop a CMP, which is applicable to all configuration items for all NARA systems, only those changes affecting NARANet, assuming system level CMPs should be sufficient; NARA is still developing a process to document and approve deviations from baseline configurations, however due to other priorities, it has not been finalized and implemented, and will take time to setup in NARA's Security Baseline Monitoring Tool. In addition, a system's (WTC) configuration management plan has not yet been developed due to inadequate ISSO oversight and ISSO learning curve.

If configuration management policies and plans are not documented, NARA's ability to adequately secure and protect its information systems could be affected. In addition, those systems without CMPs and the agency could be at potential risk for compromise.

Recommendations:
We recommend that the NARA CIO take the following actions, which include the prior unimplemented recommendations related to the weaknesses noted for the Configuration Management domain:

15. Document and implement a process to track and remediate persistent configuration vulnerabilities or document acceptance of the associated risks. (Recommendation #8 from FY2020 Financial Audit, report # 21-AUD-03)

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. (Recommendation #9 from FY2020 Financial Audit, report #21-AUD-03)

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. (New Recommendation)

18. Fully complete the migration of applications to vendor supported operating systems. (Recommendation #10 from the FY2020 Financial Audit, report #21-AUD-03)

19. 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, FY2018 FISMA Audit, report #19-AUD-02)

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

21. Document, communicate and implement NARA's configuration management processes applicable to all NARA systems, not just those under ECAB control, within NARA's CM program management plan or other NARA methodology. (New Recommendation)

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. (New Recommendation)

23. Develop and implement a configuration management plan for the WTC system in accordance with NARA's configuration management plan templates, policies, and procedures. (New Recommendation)

Metric Domain – Identity and Access Management

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

However, we noted that NARA has weaknesses in identity and access management controls in the areas of multifactor authentication, access control policy and strategy, user access requests, and account management control to include user account reviews and monitoring of inactive user accounts.

The following details the weaknesses noted in NARA's identity and access management domain.

User Authentication

OMB M-11-11[13] 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[14] 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 and 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 Threshold 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 ISSOs to perform E-Authentication risk assessments or analysis is not described within the ISSO Guide. (OFAS, ECRM, SCTS, WTC, AERIC, AERIC Title 13 and A2 PACS)[15]
- 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 NARANet 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] However, NARA has not setup a process for 164 users (who received blanket approval to become part of the debarment group, due to the pandemic) to be migrated back into 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 this is not mandatory, in conflict with OMB Memorandum M-11-11 and M-19-17 requirements. NARA has indicated there are ongoing efforts to determine funding and level of effort needed to require PIV for all privileged users and implement at the server level and 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, due to the ongoing pandemic, and related

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

[14] OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential and Access Management*.

[15] Refer to Appendix D for a description of system acronyms.

[16] The "debarment group" represents those user accounts which are not required to authenticate to NARANet using PIV.

physical access restrictions, which precluded NARA employees and contractors from obtaining a PIV card, resulting in NARA placing a large number of individuals into the PIV debarment group, so they could authenticate into the network. Further, due to NARA's ongoing determination of resource and funding requirements for this effort, NARA's full deployment of PIV for all privileged users and implementation at the server level and for all applications has been delayed.

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 systems and the agency at risk for compromise. Specifically, the lack of mandatory PIV/multifactor authentication means information system are more susceptible to attacks on user accounts.

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

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.

NARA's CFM*,* section 4.4.1.1, states ISSOs must review operating system, application, and database user accounts on an annual basis to verify that existing accounts are still valid, necessary, and that each account has the minimum necessary privileges. Additionally, ISSO's must ensure unused or inactive accounts are automatically disabled for Moderate and High Systems (manual procedures are acceptable for systems that are unable to perform this function automatically). Accounts are considered to be unused or inactive if no login has occurred within 90 days for unclassified systems and 30 days for classified systems.

NARAs processes, policies and procedures related to ICAM and user account management to include rules of behavior, removal of user accounts upon separation, inactive user account management, and user access recertifications need to be strengthened. Specifically, we noted the following weaknesses related to ICAM:

- NARA has not developed a comprehensive ICAM policy or strategy, which includes the establishment of related standard operating procedures (SOPs), identification of stakeholders, communicating relevant goals, task assignments, and measure and reporting progress. Although an ICAM Governance PowerPoint has been developed.
- NARA has not developed milestones for how it plans to align with federal initiatives, including strong authentication, federal ICAM architecture, OMB M-19-17, and phase 2 of DHS CDM program.

The following weaknesses were noted in relation to user account management:

- For 4 of 5 new hires sampled, rules of behavior were not completed/acknowledged prior to being granted system access, as part of initial security awareness training, which was also not completed during FY 2021.
- For 4 of 10 sampled systems, annual user access recertifications were not performed. No documentation was provided which demonstrates user access reviews were performed for the AERIC Title 13 system, and only user access request forms were provided for the A2 PACS, AERIC and SCTS systems.[17]
- A total of 10 user system accounts were not disabled after an employee's separation of employment for users with access to ECRM, NARANet, OFAS, and SCTS systems.[21]
- We noted that 3 network user accounts were logged into between 6 and 172 days after the employee's separation date.
- For 3 of 10 sampled systems, user accounts were identified which had either not logged in or had not logged in for more than 90 days and were not disabled or deleted. (ECRM, NARANet and ENOS)[21]

Information Services has not made it a priority to develop a formal ICAM program/governance structure, establish related policies and procedures, identification of stakeholders, communicate objectives and goals, assign tasks, and measure and report related progress, thus these efforts are still in process.

Due to inadequate ISSO oversight, system accounts were permitted to be created without a completed rule of behavior, were not reviewed, and were not disabled in a timely manner. Some of these user accounts belonged to separated employees who were included on a "do not disable" list, however they were not subsequently removed from the listing with their accounts disabled. Also, inactive user accounts partially attributed to physical access restrictions to NARA facilities (during the pandemic), where some individuals (not assigned NARA laptops to work remotely) were unable to access Citrix to login through their workstations located in NARA facilities.

If a formal ICAM policy and strategy is not in place, along with supporting policies, procedures and assignments, there is an increased risk that user account management controls could be misinterpreted, applied inconsistently, or be inadequate.

Without regular reviews of the reasonableness of user access to information systems, there is an increased risk that user accounts which are no longer needed, or access permissions which are no longer appropriate may exist, and be subject to potential misuse or abuse.

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

Background Investigation

GAO's Standards for Internal Control[18] in the federal Government states that management periodically reviews policies, procedures and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks.

[17] Refer to Appendix D for a description of system acronyms.
[18] GAO-14-704G *Standards for Internal Control in the Federal Government*, Federal Internal Control Standards, section 12.05.

We noted however that NARA's personnel security policies, specifically NARA Directive 273, *Administrative Procedures for Security Clearances*, NARA Directive 273 *Supplement*, NARA Directive 275*, Background and Identity Verification Process for Access Privileges* and NARA Directive 276, *Employment or Service Suitability Determinations*, were still out of date, as previously reported in NARA OIG Audit on Personnel Security and Suitability Program dated June 18, 2020, report No. 20-AUD-12.

This weakness was attributed to personnel security policies which were still in process of executive management review and approval within Business Support Services, thus have not yet been finalized and implemented by the Security Management Division (BX). As a result, staff is unable to rely upon these policies to guide and direct their work and may be adhering to policies which are no longer relevant.

Recommendations:

We recommend that the NARA CIO take the following actions, in addition to addressing the prior unimplemented recommendations related to the weaknesses noted for the Identity and Access Management domain:

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). (New Recommendation)

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. (New 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. (New Recommendation)

27. Enforce mandatory PIV card authentication for all NARANet users, in accordance with OMB requirements. (New Recommendation)

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. (New Recommendation)

29. Ensure NARANet user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements. (Recommendation #1 from FY 2020 Financial audit, report #21-AUD-03)

30. Ensure account reviews are completed in accordance with Access Control IT Methodology requirements. (Recommendation #5 from FY 2020 Financial audit, report #21-AUD-03)

31. Ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy. (Recommendation #15 from FY 2018 FISMA audit, report #19-AUD-02)

32. 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 FY 2018 FISMA audit, 19-AUD-02)

Metric Domain – Data Protection and Privacy

FISMA requires organizations to establish a privacy program and related plans, policies and procedures for the protection of PII collected, used, maintained, shared, and disposed of by information systems.

Per NIST SP 800-53, revision 4, control AR-1, the organization is required to update their privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially]. Also, per NIST SP 800-53, revision 4, control AR-5, the organization is required to administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII [Assignment: organization-defined frequency, at least annually.]

However, we noted that NARA's privacy policy and procedures were outdated. In addition, the FY 2021 privacy role-based privacy training was not comprehensive as the content was incomplete and the training was not completed by all personnel having responsibility for PII or for activities that involve PII. Specifically, we noted:

- NARA privacy policies and procedures have not been updated to reflect changing conditions, controls, and processes related to the determination of whether systems are required to have a privacy impact assessment (PIA). NARA 1609, *Initial Privacy Reviews and Privacy Impact Assessments* directive was last updated in 2009. This directive requires Initial Privacy Reviews (IPR) to be performed for new systems prior to connecting the system to the NARA IT network.

  However, based upon discussions with NARA Privacy officials, NARA is moving away from IPR's to be replaced by the business needs and cases as part of the Capital Planning and Investment Control (CPIC) governance process to determine whether PII exists. Thus, the NARA 1609 directive does not accurately reflect current privacy practices related to IPRs.

- NARA did not provide targeted privacy role-based privacy training during FY 2021 to all personnel having responsibility for PII or for activities that involve PII. Specifically, the extent of role-based privacy training was limited to the NARA specialized role-based training, entitled *NARA Tier II Training for System Owners (SO)'s, ISSO's and Information Services (IS) Staff*. However, this training did not include information pertaining to individual responsibility for the security and protection of PII, although there was an update related to the revised PIA format.

Without updated privacy policies and procedures, or comprehensive role-based privacy training, there is an increased risk that PII may not be adequately identified and protected from loss or misuse.

Recommendations:
We recommend that the NARA CIO with the Senior Agency Official for Privacy (SAOP) take the following actions, in addition to addressing the prior unimplemented recommendations related to the weaknesses noted for the Data Protection and Privacy domain:

33. The SAOP review and update the "*NARA 1609 Initial Privacy Reviews and Privacy Impact Assessments*" privacy policies and procedures to reflect NARA's current processes and controls. (New Recommendation)

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. (New Recommendation)

Metric Domain – Security Training

FISMA requires all federal government personnel and contractors to complete annual security awareness training that provides instructions on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot ensure that personnel would have the knowledge required to ensure the security of the information systems and data.

NARA's CFM, section 3.25.2 Security and Privacy Awareness Training, requires all new NARA personnel, as well as contractors, volunteers, students, and National Archives Foundation and Library support foundation staff must complete an initial security awareness training by reading the IT security threats and the NARA rules of behavior for access to IT resources within the first 15 days of being issued a network account.

While NARA has made improvements in their training completion rates since FY 2020, additional strengthening of controls in this area are still needed. Specifically, weaknesses were previously noted, in the identity and access management domain, regarding the completion of training for new hires as well as under the data protection and privacy domain, related to the completion of role-based training and training content.

However, for 4 of 5 new hires sampled, their initial security awareness training during FY 2021 was not completed as documented in the identity and access management domain section of this report. Also, refer to the role-based training related weaknesses noted within the data protection and privacy domain section of this report.

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:

For FISMA recommendations related to the weaknesses noted in the Security Training domain, refer to the Identity and Access Management and Data Protection and Privacy domain areas above.

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 adequately 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 on an annual frequency.

An integral part of information security continuous monitoring is the oversight of supply chain risk management. However, we noted that NARA had not yet developed and implemented a strategy to address supply chain management related risks. NARA did not document the new Authorizing Official acknowledgment of the risks to current systems, when a change in Authorizing Official occurred. In addition, not all systems had a completed annual security control assessment. Also, not all controls which had failed other control assessments, resulted in the creation of a POA&M items for tracking purposes.

Refer to authorization and accreditation, system security plan, and security control assessment weaknesses noted within the Security Assessment and Authorization 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 function refer to the Risk Management domain area above.

Security Function: Respond

Overview

NARA has defined and communicated an updated enterprise level incident response plan, utilizes 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 has been defined, communicated, and describes roles and responsibilities for the timely reporting and handling of incidents. 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 in order to demonstrate a consistently implemented maturity level.

Recommendations:

No recommendations are being made for the Respond function.

Security Function: Recover

Overview

NARA has, for the most part, 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."

Although the NARA CFM indicates that functional tests will be performed for those systems with a "Moderate" 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 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 5 of 10 sampled systems had "tabletop exercises" performed as their annual contingency plan test. However, given their assigned FIPS 199 Availability rating of "Moderate," contingency plan testing should have been "functional exercises," as required by NARA's Information Services policy and procedure document entitled "NARA CyberSecurity Framework Methodology: Processes & Procedures," specifically Section 6.5.3, Test, Training and Evaluations (TT&E) Program Summary, for "Moderate impact" systems. (A2 PACS, ENOS, NARANet, OFAS, and RCPBS)[19]

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 lack of ISSO oversight, and NARA's requirements for contingency plan testing were inconsistent, subject to interpretation.

[19] Refer to Appendix D for a description of system acronyms.

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 that the NARA CIO take the following actions related to the weaknesses noted for the Contingency Planning domain:

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. (New Recommendation)

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. NARA is generally structured with four 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 is in charge of the Office of Chief of Financial Officer, Office of Chief Acquisition Officer, Information Services, Business Support Services, and Office of Human Capital.

NARA's Information Services Office is led by the Executive for Information Services/Chief Information Officer. Information Services manages NARA's nationwide information and telecommunications infrastructure and provides oversight for NARA information systems. Information Services oversees NARA's IT security and applied research initiatives; manages NARA's IT management processes and IT governance boards; and supports the Office of Innovation in meeting customers' needs for effective and innovative social media, open government, and digitization services, solutions, and systems. Information Services also includes NARA's Chief Technology Officer, as well as a Quality Assurance Division and the Digital Preservation operations unit.

NARA operations rely on 50[20] FISMA reportable information systems hosted both internally and externally. Total IT spending by NARA represents an annual investment of approximately $99 million.[21]

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 that (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.

[20] Based upon a master system inventory listing of all NARA operational FISMA reportable systems as of 2/11/2021.

[21] https://itdashboard.gov/drupal/summary/393, 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 2021 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for federal agencies to report to OMB and, where applicable, DHS. Accordingly, the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[22]

The FY 2021 metrics are based on a maturity model approach and align to the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 3**. The FY 2021 metrics include a new SCRM domain within the Identify function area; however, the SCRM domain was not considered in the Identify framework function rating.

Table 3: Aligning the Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management[23]
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

[22] https://www.cisa.gov/publication/fy21-fisma-documents

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

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* or above.

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 GAGAS. 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 66 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. As documented in Table 4 of Appendix A, 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 the 12-month period between October 1, 2020 and September 30, 2021. 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. Refer to Appendix E for the specific systems selected for testing.

In addition, the audit included an assessment of effectiveness for each of the nine FY 2021 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.[24]

Audit fieldwork was performed during the period of April 2021 through September 2021.

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, and continuous monitoring plan.

[24] Refer to Appendix C for the current status of prior year FISMA report recommendations.

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

NARA's population of systems includes 50 FISMA reportable systems as of February 11, 2021, 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.

In addition, we leveraged the results of vulnerability assessment and penetration testing as part of the FY 2021 NARA financial statement audit of NARANet, RCPBS and OFAS systems. All three systems are in scope 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.

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

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

- OMB and DHS, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal 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 800-53A*,* Revision 4, *Assessing Security and Privacy Controls in Federal 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, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*
- OMB A-130, *Managing Information as a Strategic Resource.*
- Public Law 115-390 - *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 FY 2021. Based upon these efforts, we determined that all 24 open recommendations from prior FISMA reports were determined still open as of September 30, 2021.

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 2016, 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.
4	The CIO should develop, update, and implement formalized access control policies and procedures for the B&A, RRS, SCTS and DCU systems.
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 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 the network, RRS, B&A, ENOS-HMS and DCU 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 National Archives and Records Administration's Compliance with the Federal Information Security Modernization Act, 12/21/2018

Number	Recommendation
1	Ensure complete security authorization packages for each major application and general support system are completed prior to deployment into production.
2	Ensure SSPs are developed for all NARA systems in accordance with NARA policy.

Fiscal Year 2018, OIG Report Number 19-AUD-02
Audit of National Archives and Records Administration's Compliance with the Federal Information Security Modernization Act, 12/21/2018

Number	Recommendation
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.
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.
9	Assign ISSO's for all major applications and general support systems.
12	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.
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."
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.
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.
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.

Appendix D: Representative Subset of Sampled Systems

	System Acronym	System Name	Impact Level	Contractor System
1	A2 PACS	Physical Access Control System	Moderate	No
2	AERIC	Archival Electronic Records Inspection and Control	Moderate	No
3	AERIC Title 13	Archival Electronic Records Inspection and Control	Moderate	No
4	ECRM	Enterprise Customer Relationship Management	Moderate	Yes
5	ENOS/HMS	Expanding NARA Online Services/Holdings Management System	Moderate	No
6	NARANet	NARA Network	Moderate	No
7	OFAS	Order Fulfillment and Accounting System	Moderate	No
8	RCPBS	Records Center Program Billing System	Moderate	No
9	SCTS	Security Clearance Tracking System	Moderate	Yes
10	WTC	Websites to the Cloud	Moderate	Yes

Appendix E: Acronyms

AO	Authorizing Official
ATO	Authorization to Operate
BIA	Business Impact Analysis
BX	Security Management Division
CA	Certification and Accreditation
CCB	Change Control Board
CDM	Continuous Diagnostics Management
CFM	Cyber Security Framework Methodology
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLA	CliftonLarsonAllen LLP
CMP	Configuration Management Plan
COVID	Coronavirus Disease
CPIC	Capital Planning and Investment Control
DHS	Department of Homeland Security
ECAB	Enterprise Change Advisory Board
ETA	E-Authentication Threshold Analysis
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
ICAM	Identity, Credential and Access Management
IG	Inspectors General
IPR	Initial Privacy Review
IS	Information Services
ISCM	Information Security Continuous Monitoring
ISM	IT Security Monitoring and Authorization Branch
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OFR	Office of Federal Register
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plans of Actions and Milestones

RMF	Risk Management Framework
RTO	Recovery Time Objective
SA&A	Security Assessment and Accreditation
SAR	Security Assessment Report
SCRM	Supply Chain Risk Management
SO	System Owner
SOP	Standard Operating Procedure
SSP	System Security Plans
TT&E	Test, Training and Evaluations
US-CERT	United States Computer Emergency Readiness Team

Appendix F: Agency Comments

An exit conference was held with the agency on December 14, 2021. Prior to this meeting, agency management reviewed a discussion draft and provided comments that have been incorporated into 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 G: Report Distribution List

Archivist of the United States

Deputy Archivist of the United States

Chief Operating Officer

General Counsel

Deputy Chief Operating Officer

Chief of Management and Administration

Chief Information Officer

Accountability

Government Accountability Office

United States House Committee on Oversight and Government Reform

Senate Homeland Security and Government Affairs Committee

OIG Hotline

To report fraud, waste, or abuse, please contact us:

Electronically: https:www.archives.gov/oig/referral-form/index.html

Telephone: 301-837-3500 (Washington, D.C. Metro Area)
1-800-786-2551 (toll-free and outside the Washington, D.C. metro area)

Mail: IG Hotline
NARA
P.O. Box 1821
Hyattsville MD 20788-0821