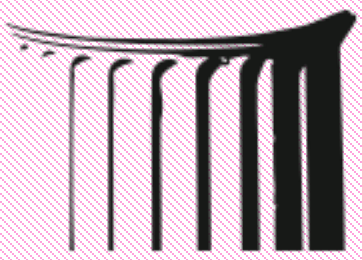

OFFICE *of*
INSPECTOR GENERAL
NATIONAL ARCHIVES

Audit of NARA's Classified Information Systems

December 12, 2019

OIG Audit Report
No. 20-AUD-03

Due to the sensitive nature of the content of this report, public release of the entire report may put systems at additional risk. The following is a summary of the report and a redacted response by NARA management.

Executive Summary

Audit of NARA's Classified Information Systems

OIG Audit Report No. 20-AUD-03 December 12, 2019

Why Did We Conduct This Audit?

As the nation's record keeper, the National Archives and Records Administration (NARA) receives classified records in both electronic and analog formats, which are then processed and stored on various classified systems. Classified systems are subject to specialized protection requirements by law.

The Office of Inspector General (OIG) conducted this audit to determine whether NARA's classified systems are adequately managed and secured in accordance with federal and NARA policies and guidelines.

What Did We Recommend?

We made 12 recommendations to strengthen NARA's security controls for classified systems in order to protect the confidentiality, integrity, and availability of the systems and data, and also bring them to conformity with federal and internal requirements and guidelines. Management concurred with the 12 recommendations in this report, and in response, provided a summary of their proposed actions.

What Did We Find?

NARA has a longstanding material weakness in internal controls over information technology (IT) security as highlighted by previous OIG audits and the agency's financial reports. Consistent with the results of our previous audit, *Audit of NARA's Classified Systems* (OIG Audit Report No. 12-15, July 23, 2012), we again found classified systems are not adequately managed and secured.

NARA does not maintain proper Authorization-to-Operate (ATO) and lacks an effective Information Security Continuous Monitoring (ISCM) program for its classified systems. The ATOs for classified systems sampled were either severely outdated or had not been issued at all. This occurred because NARA is not adhering to National Institute of Standards and Technology (NIST) nor its own policy that require ATOs to be issued and updated periodically. By not ensuring classified systems are properly authorized to operate based on a well-established continuous monitoring program, these systems may be at a significantly higher risk of containing unidentified security vulnerabilities, which could potentially allow unauthorized disclosure or misuse of national security-related information stored or processed on the systems.

Additionally, we identified multiple internal control weaknesses in the management of NARA's classified systems. Specifically, integral components of Information System Contingency Planning (ISCP) were missing; a complete and accurate system inventory was not maintained; and proper physical and environmental controls were not always in place. These conditions exist due to a general lack of management oversight and coordination by the Offices of Information Services and Business Support Services, as well as the system owners. As a result, NARA is hindered in its ability to identify and reduce the vulnerabilities and control failures associated with its classified systems, which potentially places the confidentiality, integrity, and availability of classified information at risk.

Appendix C – Management Response

NATIONAL ARCHIVES

Date: DEC 09 2019

To: James Springs, Inspector General

From: David S. Ferriero, Archivist of the United States

Subject: Management's Response to OIG Report 20-AUD-03, *Audit of NARA's Classified Information Systems*

Thank you for the opportunity to provide comments on this final report. We appreciate your willingness to meet and clarify language in the report.

As the corrective actions involve all classified systems that require substantial work with limited resources and collaboration with various system owners and business units, the target completion dates identified are beyond one year.

We concur with the 12 recommendations in this audit, and in response, the attachment provides a summary of our proposed actions. As each recommendation is satisfied, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.

DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES and
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

Action Plan Response to OIG Report 20-AUD-03,

Audit of NARA's Classified Information Systems

Recommendation 1: We recommend the Chief Information Officer review Authorizations-to-Operate (ATOs) for all classified systems at NARA that are currently in production to identify the ones that are missing, expired, or outdated, and take steps to either issue or update the ATOs for non-Sensitive Compartmented Information (SCI) systems or work with Central Intelligence Agency (CIA) to authorize SCI systems, as appropriate.

Planned Action: IT Security (IS) will perform the following actions:

- Conduct a gap analysis of all classified systems in production to identify resources necessary for the Assessment and Authorization (A&A) effort, as well as security documentation to be developed or updated prior to the security assessment and the ATO decision. (December 31, 2020)
- Prepare a schedule, for SCI systems, for A&A efforts in coordination with the CIA. (December 31, 2020)
- Complete all authorization documentation needed for security testing of non-SCI and SCI systems (December 31, 2021)
- Complete security assessment and issue ATO for all non-SCI systems and, to the extent possible, all SCI systems (December 31, 2022)

Target Completion Date: December 31, 2022

Recommendation 2: We recommend the Chief Information Officer to develop and implement a continuous monitoring strategy for all classified systems in production to effectively support ongoing authorization of the systems and to ensure security documentation for the systems always remain up-to-date.

Planned Action: IS will perform the following actions:

- [redacted] complete a master inventory of classified systems. (December 31, 2020)
- [redacted]

Target Completion Date: December 31, 2021

Recommendation 3: We recommend the Chief Information Officer ensure Information System Contingency Plans (ISCPs) for all classified systems are reviewed for accuracy and completeness and updated as necessary, at least on an annual basis.

Planned Action: IS will perform the following actions:

- [redacted] complete a master inventory of classified systems. (December 31, 2020)
- Conduct a gap analysis to determine the status of all ISCPs, and identify resources needed to support the creation of the plans or updates to the plans. (December 31, 2021)
- Create or update the ISCPs. (December 31, 2022)

Target Completion Date: December 31, 2022

Recommendation 4: We recommend the Chief Information Officer ensure contingency training and contingency plan testing are conducted for all classified systems in accordance with federal requirements and NARA policy, at least on an annual basis.

Planned Action: IS will perform the following actions:

- [redacted] complete a master inventory of classified systems. (December 31, 2020)
- Conduct a gap analysis to determine the status of all ISCPs, and identify resources needed to support the creation of the plans or updates to the plans. (December 31, 2021)
- Create or update ISCPs per recommendation 3. (December 31, 2022)
- Conduct annual ISCP training and contingency plan testing for all classified systems. (December 31, 2023)

Target Completion Date: December 31, 2023

Recommendation 5: We recommend the Chief Information ensure backup and backup testing procedures are developed, formally documented, and implemented for all classified systems.

Planned Action: IS will perform the following actions:

- [redacted] complete a master inventory of classified systems [redacted] (December 31, 2020)
- Conduct a gap analysis to identify information backup needs, as well as resources to support backups and backup testing for the classified systems. (December 31, 2021)
- Develop system-specific backup plans and test procedures for each classified system. (December 31, 2022)
- Conduct backup testing for each classified system. (December 31, 2022)

Target Completion Date: December 31, 2022

Recommendation 6: We recommend the Chief Information Officer ensure need analyses are conducted for alternate storage and processing sites, based on the Federal Information Processing Standard Publication-199 categorization and results of the Business Impact Analyses, for all classified systems.

Planned Action: IS will perform the following actions:

- [redacted] complete a master inventory of classified systems [redacted] (December 31, 2020)
- Conduct a gap analysis of the classified systems FIPS 199 and BIA documents status and identify resources to update or create them as needed. (December 31, 2021)
- Create or update ISCPs per recommendation 3 and backup plans per recommendation 5. (December 31, 2022)
- Create or update FIPS 199 and BIA based on the approved schedule. (December 31, 2022).
- Conduct an alternate storage/processing needs analysis of the classified systems, based on FIPS 199, BIA, [redacted]. (March 31, 2023)

Target Completion Date: March 31, 2023

Recommendation 7: We recommend the Chief Information Officer ensure all necessary agreements and resources are established for alternate storage and processing sites that are not susceptible to the same hazards as the primary sites, based on the results of the need analyses conducted from Recommendation 6.

Planned Action: In conjunction with the planned action to address Recommendation 6, IS will work with individual system stakeholders to determine the requirements for alternate processing and backup storage sites for their respective systems, and to develop solutions and any necessary agreements for the establishment of those sites.

Target Completion Date: March 31, 2023

Recommendation 8: We recommend the Chief Information Officer, in coordination with Business Support Services, develop and implement a process to ensure all computing resources storing or processing classified data at NARA are reported to and accurately accounted for by the Office of Information Services, including standalone workstations that are not officially categorized as a system, to ensure adequate security controls are implemented based on the classification level of the data handled by them.

Planned Action: The Capital Planning and Investment Control team will conduct a gap analysis using individual classified system inventory lists provided by Business Support Services and IS. These lists will be reconciled and used to update the Master Systems List (MSL). IS and Business Support Services will establish a repeatable process to track, review, and account for all computing resources/systems in classified work areas.

Target Completion Date: April 30, 2020

Recommendation 9: We recommend the Chief Information Officer conduct all necessary analyses to complete the required information in NARA's master system inventory, including the Federal Information Processing Standard Publication-199 categorization and classification level of the systems, and accurately reflect the results on the master system inventory.

Planned Action: IS will perform a gap analysis of the current MSL to ensure the systems listed are accurate and all security data fields including the FIPS 199 are complete in the MSL.

Target Completion Date: March 31, 2020

Recommendation 10: We recommend the Chief Information Officer, in coordination with Business Support Services, develop and implement a process to accurately record, track, and review physical locations of computing resources handling classified information.

Planned Action: I and Business Support Services will collaborate to develop a process to record, track and review physical locations of all computing resources used in classified areas. Business Support Services will provide information on classified computing resources to IS. IS will reconcile the list and update the MSL as necessary.

Target Completion Date: August 30, 2020

Recommendation 11: We recommend the Chief Information Officer, in coordination with Business Support Services, ensure physical and environmental protection controls for the facilities housing classified computing resources are assessed in accordance with NARA policy and federal requirements.

Planned Action: IS will coordinate with Business Support Services to:

- [redacted] complete a master inventory of classified systems [redacted] (December 31, 2020)
- Perform a gap analysis of the Physical and Environmental Protection (PE) controls based on CNSSI 1253, NIST, and NARA policy. (March 31, 2021)
- Develop a PE controls assessment checklist tailored for the classified facilities. (March 31, 2021)
- Conduct assessments of classified facilities using the checklist. (December 31, 2022)

Target Completion Date: December 31, 2022

Recommendation 12: We recommend the Chief Information Officer, in coordination with Business Support Services, take corrective action on the physical and environmental protection controls found to be in nonconformity with National Institute of Standards and Technology and NARA Enterprise Architecture, from the assessments conducted from Recommendation 11.

Planned Action: After completion of the planned actions to address Recommendation 11, IS will coordinate with Business Support Services to develop a Plan of Action and

Milestones for corrective action for any PE control weaknesses identified in the PE control PE controls assessments conducted for classified facilities.

Target Completion Date: March 31, 2023

Appendix D – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief of Management and Administration
Chief Information Officer
Chief Operating Officer
Deputy Chief Operating Officer
Executive for Business Support Services
Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee

OIG Hotline

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

Electronically: OIG Hotline Referral Form

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