OFFICE of
INSPECTOR GENERAL
NATIONAL ARCHIVES

October 31, 2019

TO: David Ferriero
Archivist of the United States

FROM: James Springs James Springs
Inspector General

SUBJECT: FISMA Fiscal Year (FY) 2019 OIG Narrative
OIG Report No. 20-R-01

The Federal Information Security Modernization Act of 2014 (FISMA) requires the National Archives and Records Administration (NARA) to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems supporting the operations and assets of the agency. This includes systems provided or managed by another agency, contractor, or other source. FISMA also requires an annual independent evaluation of the effectiveness of NARA's information security practices. This narrative and the responses submitted to the Office of Management and Budget (OMB) through the CyberScope portal provide our independent evaluation as to the effectiveness of NARA's information security program. We completed our evaluation in accordance with FISMA, OMB Memorandum M-17-05, and Department of Homeland Security (DHS) Fiscal Year (FY) 2019 Inspector General (IG) FISMA Reporting Metrics (the Metrics). The Metrics consist of eight domains that align with five Cybersecurity Framework Security Functions, as highlighted below.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains
Identify	• Risk Management
Protect	• Configuration Management • Identity and Access Management • Data Protection and Privacy • Security Training
Detect	• Information Security Continuous Monitoring
Respond	• Incident Response
Recover	• Contingency Planning

The Metrics require Offices of Inspectors Generals (OIGs) to assess the effectiveness of an agency's information security program on a maturity level spectrum in which the foundation levels ensure sound policies and procedures, and the advanced levels capture the extent that agencies have institutionalized those policies and procedures. Maturity levels assigned to individual Metrics ranged from "Ad-hoc," for not having formalized policies, procedures, and strategies; to "Optimized," for fully institutionalizing sound policies, procedures, and strategies across the agency. In addition, the Metrics emphasize communication and dissemination of formalized agency-wide policies and procedures. For maturity levels assigned as Defined, the OIG's review of relevant documentation was limited solely to determining if the documentation satisfied the context of the metric question.

Although NARA relies heavily on the Cybersecurity Framework Methodology (CFM) as its documented methodology for meeting FISMA requirements, NARA does not have evidence to support many of the statements documented within the CFM. Due to this, in part, and lack of Information System Security Officers (ISSO) for some systems, NARA continues to receive "Ad-hoc" maturity levels for many of the metrics.

Highlights of key observations pertaining to the formalization, communication, and dissemination of policies and procedures include the following.

- Information Services did not follow the process documented in NARA Directive 111 for developing or updating policy documents, including the CFM.
- NARA Directive 804, *Information Technology (IT) Systems Security*, has not been updated since 2007.
- References to updated criteria in NARA's CFM and other revised methodologies contradict NARA Directive 804.
- ISSO were not assigned to all systems under review during FY 2019.
- Several major applications were placed in a production environment without formal Authorization-to-Operate (ATO). Most of these systems also lacked other significant security documentation (system security plans, risk assessment reports, security assessment reports and plans of action and milestones).

The following sections highlight additional observations from this year's evaluation, grouped by the cybersecurity framework security functions indicated above.

Identify – Risk Management

We found NARA made improvements in its risk management function for this review period by broadening its identification of risks in its Risk Management Framework (RMF) Dashboard to incorporate more systems. NARA also improved its system inventory capabilities resulting in a more accurate inventory than in prior years. However, NARA has not included system interconnections within the inventory as required by 44 United States Code § 3505(c).

We also found NARA has not developed an action plan and outlined its processes to address the supply change risk management strategy and related policy and procedural requirements of the

Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technology Act). NARA also does not maintain interconnection agreements for all systems; and hardware and software inventories were inconsistent and not maintained for all systems. While ISSO play a key role in ensuring documentation and maintenance of current inventories of information system hardware and software components, not all systems have ISSO in place.

Finally, NARA did not communicate the roles and responsibilities documented in the CFM to all stakeholders involved in the risk management process nor did they communicate risks in a timely manner to stakeholders.

Protect – Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training

Although NARA has consistently implemented its Trusted Internet Connections and critical capabilities, the agency has not documented an enterprise-wide configuration management process and has not developed an Enterprise-wide Configuration Management Plan. For example, NARA's CFM, which is considered an enterprise-wide policy by Information Services, only references the Enterprise Change Advisory Board (ECAB) even though there are other Change Control Boards (CCB) in use throughout NARA. NARA will need to make necessary improvements to Configuration Management in order to be in compliance with FISMA requirements.

Improvements are also needed in NARA's identity and access management. NARA has not developed an identity, credential, and access management (ICAM) strategy. Additionally, documentation was not provided to support privileged account reviews for all systems. This issue can be directly tied to a lack of ISSO support as two of the systems for which no support was received, were also those without assigned ISSO. Additionally, the documented process for completing and maintaining access agreements is inconsistent between the various methodologies NARA has developed. Finally, E-authentication risk assessments have not been completed for NARA systems.

Although NARA has defined its organization-wide security awareness and training program, documentation was not provided to support management oversight and follow up to ensure training is completed and documented by required individuals in a timely manner.

Detect – Information Security Continuous Monitoring (ISCM)

Improvements are needed in NARA's Information Security Continuous Monitoring (ISCM) program in order to be in compliance with FISMA and the agency's internal policies and procedures. NARA needs to develop and implement an effective ISCM strategy that actively incorporates the severity of risk factors at both the agency and information system level. NARA also lacks current risk assessment reports for over a half of the systems in the sample. The National Institute of Standards and Technology (NIST) defines ISCM as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Without an effective incorporation of risk factors into the ISCM program, NARA may not be able to identify and act upon organizational or system-level risks in a timely and proactive manner. In addition, while there are several information security monitoring tools in place at NARA, the tools have not been consistently implemented across the agency to support the ongoing security monitoring and authorization of the systems. Six of the systems in the sample are currently in the production environment without a formal ATO, most of which also lack other significant security documentation such as the system security plans, risk assessment reports, security assessment reports and plans of action and milestones.

Response – Incident Response

NARA made progress and improved its incident response program. Information Services utilizes several tools in its incident response program which provide 24/7 monitoring capability for NARA's network. However, given the services in place and the amount of contractors and teams involved, NARA will need to improve its coordination and the interoperability of these services, so that communication and information sharing methods are better defined and implemented. NARA will also need to improve its process so that information is better communicated to external shareholders.

Recover – Contingency Planning

NARA has yet to establish a more mature contingency planning program. NARA does not always prepare, review, and test system-level contingency plans to ensure accurate and complete information is contained for a timely restoration of the systems and services after a disruption. Although organizations determine the recovery criticality, resource requirements, and recovery priorities based on the outage impacts and estimated downtime identified through Business Impact Analyses (BIA), a BIA was either not prepared or reviewed for at least a half of the systems sampled. This is concerning because results from the BIA are incorporated into the analysis and strategy development efforts for not only the system-level contingency plans, but also for the organization's Continuity of Operations Plan, Business Continuity Plans and Disaster Recovery Plans.

Although NARA policy requires the system security plans to document how contingency planning controls are implemented for each system based on the outage impact and recovery objectives in the BIAs, system security plans for four of the 10 systems in the sample were not finalized. Further, NARA has not fully established contingency planning strategies for cloud systems. No specific technical considerations are documented for the systems hosted in the cloud environment in NARA's IT Security Methodology for Contingency Planning, and no contingency plan was provided for the cloud-based system in the sample.

Summary and Conclusion

NARA continues to stress their commitment to improving information security throughout the agency and is making steady progress to that end. NARA also continues to work to address open OIG audit recommendations related to its information security program.

NARA made several noteworthy improvements during FY 2019 throughout the domain areas, which have been recognized in the IG metric responses as relevant and applicable:

- Through the addition of ISSO, NARA's development and maintenance of system security documentation generally improved.
- NARA broadened its identification of risks by improving its RMF Dashboard to incorporate more systems.
- NARA improved its system inventory reporting.

To fully progress towards consistently implemented, NARA needs to improve its identity and access management capability by 1) developing and implementing an ICAM strategy; 2) ensuring privileged account reviews are conducted; and 3) ensuring the completion of system E-authentication risk assessments.

In addition, NARA also needs to provide better management oversight and follow up to ensure training is completed and documented by required individuals in a timely manner and work to improve its contingency planning function to ensure it completes and tests its system-level contingency plans, conducts system BIAs, and establish contingency planning strategies for cloud systems.

The content of this narrative was shared with NARA's Office of Information Services. The results of our evaluation and this narrative were submitted within Cyberscope as required. We appreciate the cooperation and assistance NARA extended to my staff during the evaluation. Please call me with any questions, or your staff may contact Jewel Butler, Assistant Inspector General of Audits, at (301) 837-3000.