OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

DATE: October 25, 2017

FROM: James Springs
Inspector General

TO: David Ferriero
Archivist of the United States

SUBJECT: FISMA Fiscal Year (FY) 2017 OIG Narrative

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 assessment 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) FY 2017 Inspector General (IG) FISMA Reporting Metrics (the Metrics). The Metrics consisted of seven metric domains, and align with five Cybersecurity Framework Security Functions, as highlighted below.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2017 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify	• Risk Management
Protect	• Configuration Management • Identity and Access Management • Security Training
Detect	• Information Security Continuous Monitoring
Respond	• Incident Response
Recover	• Contingency Planning

The Metrics required IGs to assess the effectiveness of information security programs 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. Assessment 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 emphasized communication and dissemination of formalized policies and procedures across the agency.

Our assessment found NARA made the following improvements during FY 2017 throughout the domain areas, which have been recognized in the IG metric responses as relevant and applicable:

- NARA's Office of Information Services created the Cybersecurity Framework Methodology (CFM) in order to record its repeatable policies and procedures.
- Through the addition of Information System Security Officers (ISSO)'s, NARA's development and maintenance of system security documentation generally improved.
- NARA broadened its identification of risks by improving its Risk Management Framework (RMF) Dashboard to incorporate more systems.
- NARA's implementation of a scanning and monitoring service allowing 24/7 network monitoring capability.

While the above improvements were recognized, the emphasis on communication and dissemination of formalized policies and procedures resulted in many of the metrics receiving an "Ad-hoc" maturity level. Highlights of key observations pertaining to the formalization, communication, and dissemination of policies and procedures include:

- NARA provided the CFM as its response to most of OIG's metric questions; however, it did not ensure the CFM was disseminated to agency staff, in accordance with NARA Directive 111, *NARA Directives*.
- Information Services did not follow the process documented in NARA Directive 111 for developing or updating policy documents, including the CFM.
- NARA's Office of Information Services introduced the CFM late in the evaluation period, August 3, 2017; however, little to no evidence of preexisting policies and procedures before the issuance of the CFM was provided to OIG.
- NARA Directive 804, *Information Technology (IT) Systems Security*, has not been updated since 2007, and NARA's Enterprise Architecture has not been updated since 2011.
- References to updated criteria in NARA's CFM and other revised methodologies contradict NARA Directive 804 and NARA's Enterprise Architecture.

For maturity levels we 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. We made no further determinations on the overall sufficiency, competency, or usefulness of the documentation beyond the context of the metric question it addressed. The following sections highlight additional observations from this year's assessment, grouped by the cybersecurity framework security functions indicated above.

Identify – Risk Management

NARA made improvements in its risk management function for this review period. For example, NARA broadened its identification of risks in its Risk Management Framework (RMF) Dashboard to incorporate more systems. NARA should continue improvements by ensuring more timely communication of the Dashboard to ensure stakeholders receive the most current information. We also found NARA improved its system inventory capability to be more accurate than in prior years. However, since NARA's Chief Information Officer (CIO) does not have visibility into all parts of the agency's network, NARA may have additional IT systems it has yet to identify and evaluate. NARA also needs to ensure the accuracy of life cycle status in its system inventory, in order to better address the security risks unique to each phase.

In addition, NARA's development and maintenance of security documentation and assessments for cloud systems was inconsistent. NARA did not maintain interconnection agreements for its network. Also, NARA's hardware, software and software license inventories were inconsistent, and were not maintained for all systems. ISSOs play a key role in ensuring documentation and maintenance of current inventories of information system hardware and software components. However, NARA has not yet procured a new contract for FY 2018, and is experiencing a gap in ISSO services. Finally, many of NARA's risk management policies and procedures were not disseminated according to NARA policy, and referenced outdated policy.

Protect – Configuration Management, Identity and Access Management, Security Training

Although NARA has consistently implemented its Trusted Internet Connections and critical capabilities, configuration management continues to need improvements in order to comply with FISMA requirements. For example, NARA's Enterprise-wide Configuration Management Plan did not address applying configuration management requirements to contracted systems. In addition, configuration management roles, responsibilities, and policies as well as change control policies have not been disseminated to the appropriate individuals in accordance with NARA policy.

NARA also continues to need improvement in identity and access management. NARA ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically. However, NARA has not developed an identity, credential, and access management (ICAM) strategy, nor have ICAM roles, responsibilities, and policies been disseminated in accordance with NARA policy. Additionally, documentation was not provided to support privileged account reviews, or to support consistent completion of access request forms for individual systems. Finally, E-authentication risk assessments have not been completed for NARA systems.

NARA consistently implemented its organization-wide security awareness and training program. However, inconsistencies were found between individuals identified as having

significant security responsibilities and those individuals that needed to have specialized security training. Also, documentation was not provided to support the completion of an assessment of the knowledge, skills and abilities of NARA's workforce, or to support that training feedback was received. Further, as stated above, NARA's policies for security awareness and specialized security training also reference an outdated policy, and have not been disseminated in accordance with NARA policy.

Detect – Information Security Continuous Monitoring (ISCM)

In this reporting period, we found NARA made progress towards a more mature ISCM program by designating ISSOs to the systems, in charge of ensuring compliance with National Institute of Standards and Technology (NIST) guidance and NARA policy for their assigned systems. This resulted in improved development and maintenance of up-to-date security documentation for the systems sampled, compared to previous reporting periods. In addition, as stated above, NARA implemented a new cybersecurity and malware protection tool, which provides a 24/7 scanning and monitoring capability on NARA's network.

However, we found NARA still needs significant improvement in documenting, communicating, and implementing its ISCM policies and procedures at both the organization and information system levels, in order to meet the requirements for a maturity level of Defined or above. Not only were NARA's overarching IT security policy and supplements either outdated or not communicated in accordance with NARA policy as stated above, system-specific security plans did not always include implementation plans and responsible parties for security controls relevant to the systems sampled. Therefore, stakeholders may not be fully aware of their roles and responsibilities for the security of their systems. This is particularly concerning as the ISSO contract for FY 2018 has not been awarded and there is a gap in the ISSO coverage. Further, a security monitoring plan for cloud-based systems has not been fully developed, and there are inconsistencies among those systems for development and maintenance of security documentation and assessments.

Response – Incident Response

NARA made progress and improved its incident response program. Information Services utilizes several tools in its incident response program, and as mentioned prior, recently procured and implemented a service, which provides 24/7 monitoring capability for NARA's network. However, given the new services 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. In addition, NARA will need to improve its process so that information is better communicated to external shareholders, as we found that not all incidents were reported timely to US-CERT. Lastly, NARA has yet to develop and implement incident monitoring requirements for cloud-

based environments, which represents significant risk to NARA's information and systems given NARA's plans to move more applications and data storage to lower-cost, commercial hosting.

Recover – Contingency Planning

Although NARA conducts an annual, agency-wide Eagle Horizon exercise that incorporates mission-critical systems, system-level contingency plans and the tests of the plans are not always completed in accordance with NARA policy and NIST guidance. NARA has yet to establish a more mature contingency planning program. In addition, NARA has not dedicated adequate attention to conducting and updating Business Impact Analyses (BIAs) for information systems. Although NARA requires a formal, system-level BIA to be conducted because it will identify allowable down-time, we found BIAs for information systems were either not conducted or severely outdated for many of the systems sampled. Further, System Security Plans (SSPs) for systems did not always contain implementation plans for Contingency Planning (CP) controls, including alternate storage/processing sites, system backup, and system recovery and reconstitution controls.

Lastly, in August 2006, NARA signed a Memorandum of Understanding (MOU) for use of a U.S. Navy facility to support the operations of NARA's alternate operating site for its headquarters, the Electronic Records Archives (ERA) program, an alternate production site for the Federal Register, and an alternate network operation center for NARA's vital nation-wide telecommunications network including NARANet. Although this MOU expired on June 2016, it was not renewed until July 2017, which resulted in NARA occupying and utilizing the facility for the said operations without a current agreement for over one year. In addition, the unsigned version of the agreement prepared for a renewal did not include the operations of the ERA program, which was discovered during the fieldwork of a separate OIG audit which also took place in FY 2017. As many of NARA's systems rely on this facility as their alternate processing and/or storage site, it is crucial that NARA maintains an accurate and up-to-date agreement.

Summary and Conclusion

NARA continued progress on its new initiatives, aided by the ISSOs which were in place for most of the FY 2017 reporting period. However, since NARA is experiencing a gap in these services and it will take time to initiate and cycle replacement services, NARA's information security program is at increased risk. In addition, Information Services continued to experience changes in leadership, including the appointment of a new Chief Technology Officer in December 2016. Also, the organization structure of the CIO remains challenged; as the CIO does not report directly to the Archivist.

As a vital step to improving NARA's information security program, NARA will need to ensure it develops its capability to document, update, communicate, disseminate, and implement its

program policies and procedures at both the organization and information system levels. Improvements can also be made to the program function areas. For example, within its risk management program NARA should continue to develop its ability to identify and evaluate existing systems on its network in order to ensure accurate, up-to-date, and complete inventories are maintained for its systems and related components. Given current government initiatives to move to the cloud, NARA will also need to further its capabilities to provide adequate security protections for those systems and information externally hosted by contractors, including cloud computing systems.

NARA can improve its identity and access management capability by 1) developing and implementing an ICAM strategy; 2) ensuring privileged account reviews are conducted; 3) ensuring system access request forms are consistently implemented for individual systems, and 4) ensuring the completion of system E-authentication risk assessments.

NARA's security training function could better identify individuals with significant security responsibilities and those that require specialized security training. NARA can improve its posture to better gauge the effectiveness of its security and awareness training program by also improving its assessment of the knowledge, skills and abilities of NARA's workforce, and obtaining and evaluating training feedback. NARA should also work to improve its contingency planning function to ensure it completes and tests its system-level contingency plans, conducts system BIAs, and includes implementation plans for CP controls in its SSPs.

NARA continues to stress their commitment to improving information security throughout the agency and will continue to work with the OIG to ensure information security weaknesses are addressed.

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