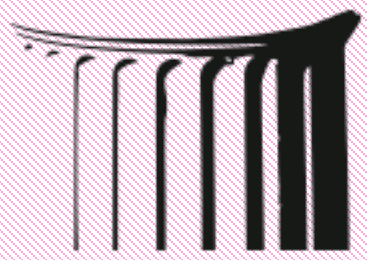

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

Federal Information Security Modernization Act of 2014
Fiscal Year 2020 OIG Narrative

October 29, 2020

OIG Report 21-R-02

OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

October 29, 2020

TO: David Ferriero
Archivist of the United States

FROM: James Springs
Inspector General

SUBJECT: Federal Information Security Modernization Act of 2014 Fiscal Year 2020 OIG Narrative
OIG Report 21-R-02

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. FISMA also requires an annual independent assessment 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 assessment in accordance with FISMA, OMB Memorandum M-20-04 *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, and Department of Homeland Security (DHS) Fiscal Year (FY) 2020 Inspector General (IG) FISMA Reporting Metrics (the Metrics). The Metrics consist of eight domains that align with five Cybersecurity Framework Security Functions.

The Metrics require Offices of Inspectors General (OIGs) to assess the effectiveness of their agencies' 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. 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.

Summary

Overall, NARA has not changed from last year, having five domains assessed at the lowest "Ad - hoc" level, and three domains assessed one level above the lowest at the "Defined" level. However, NARA continues to stress its 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 information security.

In FY 2020, NARA continued its progress toward a more mature information security program, including the following.

- Acquiring additional Information System Security Officer (ISSO) resources, which helped the agency create and maintain up-to-date security documentation for many systems in the sample.[1]
- Improving its master system inventory process to include more accurate and comprehensive system information compared to prior years.
- Introducing new channels of communication to update information security stakeholders on the newest security topics and changes in information technology (IT) policies and procedures.

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, the foundational levels of a mature information security program. The FY 2020 OIG-assessed maturity levels for each Metric Domain, compared to the FY 2019 assessment results, are included in Table 1 below.

Table 1. FY 2020 OIG-Assessed Maturity Levels for FISMA Metric Domains

Function	Identify	Protect				Detect	Respond	Recover
Domain	Risk Management	Configuration Management	Identity & Access Management	Data Protection & Privacy	Security Training	ISCM	Incident Response	Contingency Planning
OIG Assessed Maturity	Ad Hoc (Level 1)	Ad Hoc (Level 1)	Ad Hoc (Level 1)	Ad Hoc (Level 1)	Defined (Level 2)	Ad Hoc (Level 1)	Defined (Level 2)	Defined (Level 2)
Change from FY 2019	Downgraded from Defined (Level 2)	No Change	No Change	No Change	No Change	No Change	No Change	Upgraded from Ad Hoc (Level 1)

[1] The following systems were included in the sample (locations are noted in parentheses): Archival Records Center Information System (Archives II, College Park, MD); Case Management and Reporting Systems (Archives II, College Park, MD); Electronic Records Archive 2.0 (cloud-based); Microfiche Reader Modernization Project System (National Personnel Records Center, Spanish Lake, MO); NARANet (NARA locations nationwide); Order Fulfillment Accounting System (Archives II, College Park, MD); Presidential Electronic Records Library (Archives II, College Park, MD); and ZLTech Unified Archive (cloud-based).

Results

NARA's information security program has longstanding weaknesses in developing and consistently implementing policies and procedures. Although NARA relies heavily on the Cybersecurity Framework Methodology (CFM) as its documented policy for meeting FISMA requirements, it does not accurately reflect the current state of NARA's information security program in many cases. NARA indicates the CFM was written to outline the "desired state" of information security. Given this, evidence to support the current state is lacking.

There is a lack of consistency between the CFM and other NARA artifacts including the IT security architecture and methodology documents, the ISSO Handbook, and individual system security documentation describing IT security policies and procedures. The conflicting requirements and guidance resulted in 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 many of the metric questions.

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

- Policy Development
    - NARA Directive 804, *Information Technology (IT) Systems Security*, has not been updated since 2007.
    - Discrepancies were noted within the CFM or between the CFM and other policy or procedure documents discussed above.
- Implementation of Policies and Procedures
    - NARA systems do not go through a reauthorization process when there is a change in the authorizing official.
    - Systems without ISSO coverage lack proper documentation, implementation, and assessment of security controls.
    - There was a significant delay in the rollout of the annual security awareness and privacy training, resulting in a lower completion rate reported as compared to prior years.
    - Role-based privacy training has not been fully developed and deployed.
- Communication of Formalized Policies and Procedures
    - System owners are not regularly updated on changes in IT policies and procedures.
    - Annual Tier-II security training does not include topics related to new or updated policies and procedures.

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

Identify – Risk Management

NARA has improved its system inventory capabilities resulting in a more accurate inventory than in prior years. NARA has developed the CFM, the FISMA Inventory Management Standard, and the Master Systems List Management Guide that collectively establish a comprehensive system inventory process. However, these documents do not always align with one another as to who is held responsible for maintaining an accurate and complete master system inventory. In addition, inconsistencies were found within the CFM on what taxonomy fields should be included in the hardware and software inventories, and our sample testing revealed that the taxonomies maintained in the hardware and software inventories varied by system. While the ISSOs play a key role in ensuring documentation and maintenance of current hardware and software inventories of their assigned information systems, not all systems currently have an ISSO in place.

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 has not developed a risk management strategy that includes a risk profile and risk appetite/tolerance levels.

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

Configuration Management

Although NARA has consistently implemented some of its critical capabilities including the Trusted Internet Connections (TIC) and the inventory of the agency network connections, the agency continues to lack complete and consistent documentation and communication of its configuration management policies and procedures as required by FISMA. Although the CFM is considered an enterprise-wide information security policy, it only references the Enterprise Change Advisory Board (ECAB) and not the other Change Control Boards (CCB) in use throughout the agency for change management. Although system owners play an important role in identifying, defining, and ensuring implementation of all aspects of configuration management for their information systems, they are not sufficiently informed of changes in policies and procedures.

Security Training

Though NARA has defined its organization-wide security awareness training program, documentation was not provided to support management oversight and follow-up to ensure

training was completed and documented by all required users in a timely manner. The agency did not ensure funding was secured for security and awareness training in a manner that would facilitate timely rollout, resulting in a lower completion rate reported as compared to prior years.

Identity and Access Management

NARA has not developed an identity, credential, and access management (ICAM) strategy. Sufficient documentation was not provided to support privileged accounts were logged and periodically reviewed for all systems in the sample. NARA has a documented process for completing and maintaining user access agreements and requires all users to sign the rules of behavior as part of the annual security awareness and privacy training. However, we were unable to verify all users signed the rules of behavior due to the delayed rollout of the training, as discussed above.

Data Protection and Privacy

While NARA has established data protection and privacy policies and procedures at a high level, the Privacy Program has not been consistently implemented and communicated throughout the agency. NARA utilizes a number of preventative and detective tools to protect against unauthorized disclosure of sensitive information including Personally Identifiable Information (PII). However, NARA policies and procedures do not sufficiently address how these protective measures apply to each system containing sensitive information. In addition, the Privacy Impact Assessments and annual recertification of the assessments have not been consistently performed for the systems in the sample, and role-based PII training has not been fully developed and provided to the individuals who have significant responsibilities for the Privacy Program.

Detect – Information Security Continuous Monitoring (ISCM)

NARA has not developed and implemented an effective ISCM strategy that actively incorporates the severity of risk factors at both the agency and information system level. Although the ISSOs are regularly notified of changes in IT security policies and procedures, NARA system owners are not consistently notified. This puts system owners without ISSO support at a risk of not being fully aware of their ISCM roles and responsibilities based on the latest requirements and guidelines. Although there are a number of information security monitoring tools in place at NARA, they have not been consistently documented or implemented across the agency to support the ongoing security monitoring and authorization of the systems, including those previously authorized by the former authorizing officials and hosted in a cloud-based environment.

Response – Incident Response

In general, NARA has defined incident roles and responsibilities that are consistently performed by the assigned individuals. NARA's Office of Information Services utilizes several tools to provide 24/7 monitoring capability for the agency's network. However, the agency did not provide evidence to support: (1) resources are allocated in a risk-based manner for stakeholders to

effectively implement incident response activities; and (2) stakeholders are held accountable for carrying out their roles and responsibilities effectively. NARA lacks coordination between employees and contractors to carry out effective and efficient incident prevention, detection, and resolution for various systems and services for which contractors have shared management responsibilities. While NARA shares information on incident activities with various stakeholders, the agency did not provide sufficient documentation to show it complied with all incident reporting requirements to external stakeholders including the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) for this reporting period.

Recover – Contingency Planning

NARA has yet to establish a more mature and well-rounded contingency planning program. NARA does not always prepare, review, and test system-level contingency plans to ensure the accuracy and completeness of the information required for a timely restoration of the systems and services after a disruption. Policies and procedures concerning contingency plan tests and exercises have not been fully developed and implemented, resulting in inconsistent test procedures, requirements, and frequencies by system. Additionally, business impact analyses conducted for individual systems are not consistently utilized to identify and implement necessary continuity-of-operations measures to minimize the length and impact of a disruption in accordance with the mission criticality and impact level determined by the analyses.

We want to reiterate that NARA continues to stress its commitment to improving information security throughout the agency and is making steady progress to that end. The content of this narrative was shared 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.

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
Sheena Burrell, Deputy Chief Information Officer
Sandra Paul-Blanc, Chief Information Security Officer
Kimm Richards, Accountability