OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

November 9, 2016

TO: David Ferriero
Archivist of the United States
Office of the Archivist of the United States (N)

FROM: James Springs
Inspector General (OIG)

SUBJECT: FISMA Fiscal Year (FY) 2016 OIG Narrative

Each year the Federal Information Security Modernization Act of 2014 (FISMA) requires an independent evaluation of the effectiveness of the National Archives and Records Administration's (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 of the quality of NARA's information security practices.

We completed our evaluation in accordance with FISMA, OMB Memorandum M-16-03, and Department of Homeland Security (DHS) FY 2016 Inspector General FISMA Reporting Metrics, which provided the reporting instructions for meeting FISMA requirements.[1] The FY 2016 Inspector General FISMA reporting metrics consisted of eight metric domains, aligned with five Cybersecurity Framework Security Functions, as highlighted below.

Table 1. Aligning the Cybersecurity Framework Security Functions to the FY 2016 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

[1] OMB Memorandum M-16-03 indicated the annual Inspector General reporting deadline was to be determined; the FY 2016 Inspector General FISMA Reporting Metrics provided the reporting deadline of November 10, 2016.

Our assessment found NARA made significant efforts in the area of Security and Privacy Training to address some weaknesses identified in previous FISMA evaluations and audit engagements. Examples of some of these efforts include, and are not limited to the following.

- Designation of Information System Security Officers (ISSOs) to perform security support services.
- Identification of individuals with elevated security responsibilities for Tier-II security and privacy awareness training and the Logical Access Control System (LACS).
- Progress with the implementation of the Homeland Security Presidential Directive 12 (HSPD-12).
- Development and deployment of Tier-II security and privacy awareness training and the insider threat program.

As a result of NARA's efforts, we determined NARA's overall security and privacy training program was effective for this assessment period.

We found NARA still needs significant improvement in seven of the eight metric domains in order to be consistent with FISMA and National Institute of Standards and Technology (NIST) guidance. Many of the weaknesses identified from the seven metric domains pertained to underdeveloped and inconsistently implemented policies and procedures, which potentially expose the confidentiality, integrity, and availability of the agency's information and information systems to unauthorized access, use, disclosure, disruption, modification, or destruction. The following highlights some of the observations from this year's assessment, grouped by the cybersecurity framework security functions indicated above.

Identify – Risk Management and Contractor Systems

NARA made progress by designating Information System Security Officers (ISSO) in FY 2016; however the ISSOs arrived too late in the fiscal year to impact this reporting period. Though we recognize the newly designated ISSOs will assist in some of these process areas, NARA continued to struggle with weaknesses in its risk management activities during this reporting period. As this was the first contract year for these ISSOs, NARA OIG will re-evaluate the Tier-II training material and recipients of the training in the next reporting period to determine the adequacy and compliance with NARA policy and applicable NIST guidance.

Similar to prior years, NARA lacks adequate documentation of baseline security controls and did not have an accurate inventory of systems. NARA also lacked adequate categorization of its systems, and did not adequately maintain the documentation in security authorization packages necessary for ongoing authorizations. For example, plans of actions and milestones (POA&M) and risk assessments were not consistently updated; and system security plans (SSP) didn't always define the time period for review of the risk assessments, per NARA's security methodology. Some SSPs were not available, and sometimes draft documents were provided. Numerous systems we sampled, including contractor systems, did not have valid Authorizations to Operate (ATO). Interconnection agreements were not readily available for NARANet. Further, some security assessment reports were not provided.

We also found POA&MS were not consistently updated, and although NARA utilized a dashboard, quarterly POA&M reports were no longer delivered leaving NARA unable to demonstrate effective communication of risks to system stakeholders. In addition, documents important to planning and performing risk management activities need to be updated. For example, Information Services did not update its risk management strategy according to its security methodology. The strategy is signed by the prior Chief Information Officer (CIO) and isn't clear on how Information Services will address higher risk areas such as controls over contractor systems. NARA's *IT Security Methodology for Risk Assessment* had also not been updated. The last revision was in 2011.

Externally hosted contractor systems managed on behalf of a federal agency must still be FISMA compliant and undergo the same rigor for security assessments as on-premises systems. However, provision and oversight of information security controls in off-premises contractor systems harbors much greater challenges. Similar to past years, NARA did not have an up-to-date inventory of contractor-operated systems. Their current inventory may also create difficulties for future Capital Planning reporting because the agency's master listing did not consistently designate whether cloud systems are public, hybrid, or private.

Our review of documentation for security authorization packages for cloud systems showed NARA was not aligned with FISMA because not all had valid ATOs; being either outdated or unsigned. In addition, although NARA provided security authorization packages for the infrastructure of one system, the agency did not provide a similar package for the application relying upon the infrastructure, in accordance with FedRAMP requirements. In these unique environments, agreements are also critical in the successful application of controls, such as adequate service level agreements. Coordination across business areas is needed, for example between Acquisitions and Information Services. In response to a prior year FISMA recommendation, NARA has created standard language for IT contracts to address this risk. However, these standards were still in draft and not approved for this reporting period.

Protect – Configuration Management, Identify and Access Management, and Security and Privacy Training

NARA's configuration management continues to need improvements in order to be in compliance with FISMA requirements. NARA's configuration management plans for the systems sampled were either outdated or not developed. NARA also did not have an effective process for monitoring, detecting, and remediating known vulnerabilities. The FY 2016 Financial Statement Auditor's vulnerability scans found 650 critical and high severity vulnerabilities regarding patches and software updates within NARA's network environment, including missing patches dating back to 1999. Although NARA had a patch and vulnerability management program in place, it was not effective and did not result in the identification and implementation of all needed software patches and upgrades.

NARA also continues to need improvement in identity and access management. As stated above, NARA made progress with implementing the Personal Identity Verification (PIV) for logical access within this reporting period. However, NARA continues to be noncompliant with HSPD-12 for either physical or logical access control. In addition, policies and procedures for access

control and authentication were not adequately implemented. Numerous issues regarding access controls for shared or privileged accounts were revealed by the recent OIG Audit of NARA's Management Control over Microsoft Access Applications and Databases. Further, there continues to be a lack of effective communication and cooperation between the offices of Human Capital (H) and Information Services (I) regarding terminated employees and timely removal of their access to NARA facilities and information systems.

NARA developed the insider threat program and training in late FY 2015 through early FY 2016. However, the training is currently provided separately from the annual security privacy awareness training. FISMA requires training material for security and privacy awareness training to contain appropriate content for the organization, including insider threat topics. NARA currently only uses the list of individuals who are compliant with the annual requirement to take security and privacy awareness training for annual account recertification, and not the list of individuals who are compliant with the annual insider threat training requirement. In order to ensure continued compliance with FISMA requirements in future years, we strongly suggest NARA implements a process to review both lists before an annual account recertification is granted to a user.

Detect – Information Security Continuous Monitoring (ISCM)

The FY 2015 FISMA assessment determined NARA was at Level 1 - Ad-hoc for its ISCM program. In FY 2016, NARA made improvement by identifying the individuals with elevated security responsibilities and providing Tier-II security and privacy training to those individuals, as discussed above. In addition, NARA has recently awarded a security support service contract, through which it designated ISSOs to each of the systems in NARA's system inventory. However, these improvements did not take place until the end of FY 2016 through the beginning of FY 2017.

For most of this reporting period, NARA was not in compliance with the requirements to move to the next maturity level, Level 2: Defined. Specifically, NARA had not: (1) fully established and implemented security policies and procedures for the systems sampled; (2) updated, reviewed, or assessed system security plans on a periodic basis; or (3) maintained a complete and accurate system or hardware/software asset inventory. As a result, the maturity level for this metric domain remained at Level 1: Ad-hoc, consistent with last year's maturity level. With the designation of the ISSOs, in charge of ensuring compliance with NIST guidance and NARA policy for their assigned systems, we expect further improvement to NARA's ISCM program will be realized in the next reporting period and years to come.

Respond – Incident Response

NARA established an incident response and reporting program and has further established an Insider Threat Program. NARA has also implemented the Trusted Internet Connection, and utilizes DHS' Einstein and various intrusion detection and prevention tools to timely identify, respond to, and resolve computer security incidents. NARA continues to make improvements to its incident response capabilities and plans to implement a formalized Security Operations Center (SOC) in FY 2017.

Alongside this progress, NARA's limited resources have at the same time made it difficult to consistently implement incident response activities. For example, incident reporting and response is ad-hoc because NARA does not currently have a primary collection point for reporting incidents due to inconsistent and varying incident reporting methods communicated through its methodology. NARA experienced difficulty ensuring adherence to its security procedures for documenting incidents. For example, not all tickets were reported to US-CERT within one hour of the incident being reported. Incident categorizations and US-CERT information were not consistently documented in NARA's designated incident reporting system. US-CERT information was not required by the system and had to be entered manually.

NARA has yet to formally document how it will accomplish some of its incident response activities. For example, qualitative and quantitative performance measures for its incident response program, and how it will integrate incident response activities with other organizational mission/business areas such as risk management. NARA also needs to determine and document fully how it will manage incident response risks associated to its externally hosted contractor systems. NARA's 2014 incident response plan is outdated and relies upon a gap analysis from 2010. As a result, the plan no longer reflects NARA's current environment and is not consistent with existing security policy.

Recover – Contingency Planning

In FY 2016, NARA did not dedicate adequate attention to contingency planning. Specifically, Business Impact Analyses were not completed in recent years, and contingency plans for the systems sampled were outdated, incomplete, or not tested on an annual basis. This, increases the risk that restoration procedures may become irrelevant in the event of a disaster. In addition, it is NARA policy that a sample of backup information in the restoration of selected information system functions is used as part of contingency plan testing, for data requiring high availability. However, no evidence of backup restoration testing, separately from or as part of an annual contingency plan testing was provided for numerous systems in our sample. Included in these systems were those that have a FIPS-199 impact categorization of "high."

Further, NARA has identified access to the internet and email as the only mission-critical functions for continuity-of-operations (COOP) purposes in the event of an emergency. In order to effectively carry out NARA's mission to provide public access to Federal government records in our custody and control, NARA needs to ensure proper collaboration and communication take place between offices in: (1) identifying systems serving the functions critical to NARA's mission; and (2) adequately preparing them for minimal disruption of service during an emergency.

Summary and Conclusion

NARA experienced changes in leadership in information security in 2015 and 2016, including the appointment of a new Chief Information Security Officer. New initiatives have also been introduced to promote a mature information security program for the agency. However, NARA is challenged by yet another reorganization whereby the CIO is not aligned for direct reporting access to the Archivist. In order to establish an effective information security program, NARA needs to ensure it: (1) maintains up-to-date, complete, and accurate system inventory; (2) develops, formalizes, and consistently implements information security policies and procedures;

and (3) adequately allocates resources to perform and monitor security tasks, as prescribed by NARA policy and applicable laws and regulations. Specifically, NARA's underdeveloped process on defining and categorizing information systems resulted in possible omission and/or mis-categorization of information systems in its system inventory, leading to bypassing of security controls required for the type of data contained within an information system. A number of OIG audits conducted within this assessment period revealed issues regarding the accuracy and completeness of NARA's system inventory. In turn, this made it difficult for NARA to ensure all security controls have been adequately implemented to its systems and data as required by FISMA, OMB Policy, and NIST guidance.

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. I appreciate the cooperation and assistance 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.