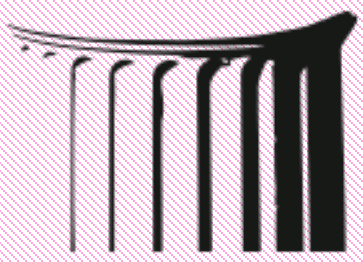


OFFICE of INSPECTOR GENERAL
NATIONAL ARCHIVES

Audit of NARA's Cybersecurity Risk Management Process

August 27, 2020

OIG Audit Report No. 20-AUD-15

Table of Contents

Executive Summary

Audit of NARA's Cybersecurity Risk Management Process

OIG Audit Report No. 20 AUD 15 August 27, 2020

Why Did We Conduct This Audit?

Federal agencies rely on information technology (IT) systems and electronic information to carry out their mission. This is especially true for National Archives and Records Administration (NARA) where information technology is an essential component of carrying out the agency's strategic plan. However, with agencies' continual reliance on IT systems, the risks to the agency and IT is only going to increase as current threats advance and new threats emerge. It is imperative that agencies implement cybersecurity risk management protections to adequately identify, prioritize and manage cyber risks.

The Office of Inspector General (OIG) conducted this audit to assess NARA's cybersecurity risk management efforts.

What Did We Recommend?

We made two recommendations to strengthen NARA's cybersecurity risk management program to include ensuring greater accountability by stakeholders; developing a risk management strategy and policy; and coordination between cybersecurity and enterprise risk management. Management concurred with the two recommendations in this report, and in response, provided a summary of their proposed actions.

What Did We Find?

NARA does not have a fully established cybersecurity risk management program. Specifically, NARA has not: (1) fully defined and communicated roles and responsibilities of Risk Executive (function); (2) developed an enterprise-wide risk management strategy; (3) documented or implemented risk-based policies; and (4) established coordination between cybersecurity and enterprise risk management. This occurred because NARA has not made it a priority to fully implement a cybersecurity risk management program. Without a complete and comprehensive cybersecurity program whereby NARA can effectively identify, prioritize, and manage cyber risks, the agency remains vulnerable to unmitigated risks that threaten NARA's information systems and IT environment.

Summary of Recommendations

Finding: NARA Does Not Have a Fully Established Cybersecurity Risk Management Program.

Number	Recommendation	Responsible Office
1	Ensure the Risk Executive, Chief of Management and Administration, Chief Operating Officer, and Senior Accountable Official for risk management roles and responsibilities are fully and accurately defined in NARA policies.	Chief of Management and Administration and Chief Operating Officer
2	Develop, document, implement, and disseminate an organizational risk management strategy and policy, in accordance with NIST 800-39, and a process for coordination between cybersecurity and enterprise risk management.	Chief of Management and Administration

Background

Federal agencies rely on information systems and electronic information, collectively known as information technology (IT), to carry out their missions. It is imperative that agencies implement cybersecurity risk management protections to adequately identify, prioritize, and manage cyber risks. This is especially true for the National Archives and Records Administration (NARA) where IT is an essential component of carrying out the 2018-2022 Strategic Plan. The Strategic Plan includes a transformational outcome that states, "NARA will embrace the primacy of electronic information in all facets of its work and position NARA to lead accordingly." According to NARA's strategic goal 3.2 "By the end of 2022, NARA will, to the fullest extent possible, no longer accept permanent or temporary records in analog formats and only accepting records in electronic format and with appropriate metadata."

As reliance on IT continues to grow, so do the risks to agencies and the systems they rely on. Those risks include insider threats, threats from foreign countries, and advancements in attack sophistication among others. According to Executive Order 13800, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* agency heads are to be held accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. Additionally, cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents.

The Office of Management and Budget (OMB) Memorandum 17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* indicates an effective enterprise risk management (ERM) program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. It further states, effective management of cybersecurity risk requires agencies align information security management processes with strategic, operational, and budgetary planning processes.

NARA's Information Services Cybersecurity and Information Assurance Division develops and manages NARA's IT Security Program, including provision for the security of information and

IT systems that support the operations and assets under their control. In fiscal year (FY) 2019 NARA had approximately $5.7 million in operating expenses allocated to cybersecurity.[1]

Several previous Office of Inspector General (OIG) audit reports reviewed cybersecurity risk management activities. The Enterprise-Wide Risk Assessment Audit of NARA's Internal Controls (OIG Audit Report No. 17-AUD-01, dated October 28, 2016) found NARA had yet to implement an enterprise-wide risk management program that clearly identifies, prioritizes, and manages risks throughout the organization and NARA management had not made the implementation of an enterprise-wide risk management program a strategic priority, which resulted in eight recommendations. As of the date of this audit report, seven recommendations remain open.

The Audit of NARA's Legacy Systems (OIG Audit Report No. 18-AUD-06, dated March 29, 2018) noted NARA had not conducted risk assessments for some of its systems, resulting in the OIG making one recommendation. As of the date of this audit report, this recommendation remains open.

The Audit of NARA's Compliance with the Federal Information Security Modernization Act (FISMA) (OIG Audit Report No. 19-AUD-02, dated December 21, 2018), identified several weaknesses within the FISMA risk management metric domain associated with the Identify function area of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including inventory listing inaccuracies, information security program weaknesses, policies and procedures issued without going through the proper approval process, and a lack of ISSOs for information systems, which resulted in nine recommendations. As of the date of this audit report, seven of the nine recommendations remain open.

In FY 2019 the OIG conducted an evaluation (OIG Audit Report No. 20-R-01, dated October 31, 2019) of NARA's compliance with FISMA. While we did not make any recommendations, we noted although NARA made improvements to its risk management function including broadening its use of the Risk Management Framework (RMF) dashboard and an improved system inventory, NARA did not maintain interconnection agreements for all systems; and hardware and software inventories were inconsistent and not maintained for all systems. While Information System Security Officers (ISSO) play a key role in ensuring documentation and maintenance of current inventories of information system hardware and software components, not all systems had ISSOs in place. In addition, NARA had not completed E-authentication risk assessments for its systems.

The Audit of NARA's Classified Information Systems (OIG Audit Report No. 20-AUD-03, dated December 12, 2019) identified that Authorization-to-Operate for NARA's classified

[1] This amount does not include cybersecurity costs for each project and system. In addition, Information Services and risk management programs are embedded activities without direct budget allocations.

systems were either severely outdated or had not been issued at all, making twelve recommendations. As of the date of this audit report, eleven of the recommendations remain open.

Objectives, Scope, Methodology

Objectives

The objective of this audit was to assess NARA's cybersecurity risk management efforts. Specifically, we reviewed NARA's efforts to develop a cybersecurity risk management program. The audit excluded cybersecurity activities evaluated during previous audits and our annual FISMA assessments, including vulnerability scanning, system risk assessments, and system authorizations.[2]

Scope and Methodology

To accomplish our audit objective, we performed audit procedures at Archives II in College Park, Maryland. This audit was performed from May 2019 to October 2019.[3]

Specifically, we performed the following.

- Reviewed NARA Directive 804, *Information Technology (IT) Systems Security*, and NARA Directive 160, *NARA's Enterprise Governance, Risk, and Compliance Program*.
- Reviewed applicable laws, regulations, and circulars.
- Conducted interviews with the Chief of Management and Administration (CMA), Chief Operating Officer (COO), and employees within Information Services to gain an understanding of NARA's cybersecurity risk management program.
- Assessed the internal controls identified to determine if the controls were sufficient to ensure NARA can effectively manage and oversee the risk management program.
- Evaluated the cybersecurity risk management roles and responsibilities, strategy, policies, and the process of communicating risks to senior management.

Internal Controls

To assess internal controls relative to our objective, we reviewed the FY 2018 and FY 2019 Assurance report for the Offices of Information Services. The Chief Information Officer (CIO) submitted a qualified statement of assurance indicating management controls of Information Services in effect during the years ending September 30, 2018 as well as September 30, 2019, were adequate and effective in ensuring that (l) programs achieved their intended results; (2) resources are used consistent with NARA's mission; (3) programs and resources are protected from waste, fraud, and mismanagement; (4) laws and regulations are followed; and (5) reliable and timely information is obtained, maintained, reported and used for decision making. We noted

[2] Identified in the five functional areas in the *NIST Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).

[3] Due to other high audit priorities, this audit was delayed.

that Information Services has identified IT security as a material weakness for four consecutive years (FY 2015 - FY 2018). We assessed the control environment in accordance with Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*. Our assessment found NARA's controls were not properly designed, implemented, or operating effectively. Specifically, management has not established activities to adequately respond to and manage cyber risks, including defining roles and responsibilities, a risk management strategy, risk-based policies, and coordination between cybersecurity and enterprise risk management.

This performance audit was conducted in accordance with generally accepted government auditing standards. The generally accepted government auditing standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit was conducted by Andrew Clements, Senior IT Auditor.

Audit Results

Finding. NARA Does Not Have a Fully Established Cybersecurity Risk Management Program.

NARA does not have a fully established cybersecurity risk management program. Specifically, NARA has not: (1) fully defined and communicated roles and responsibilities of Risk Executive (function); (2) developed an enterprise-wide risk management strategy; (3) documented or implemented risk-based policies; and (4) established coordination between cybersecurity and enterprise risk management. This occurred because NARA has not made it a priority to fully implement a cybersecurity risk management program. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, states agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. The Executive Order requires agencies to take several specific actions in order to evaluate and improve cybersecurity risk management across the executive branch. Without a complete and comprehensive cybersecurity program whereby NARA can effectively identify, prioritize, and manage cyber risks, the agency remains vulnerable to unmitigated risks that threaten NARA's information systems and IT environment.

Role of a Risk Executive (Function)

NARA has not fully defined and communicated a risk executive (function) that provides agency-wide oversight of cybersecurity risk activities and facilitates collaboration among stakeholders and consistent application of a risk management strategy. NIST SP 800-39 states agencies should establish a risk executive (function). The risk executive (function) can be filled by an individual or office (supported by an expert staff) or by a designated group within the organization.

Currently, the COO serves as NARA's Chief Risk Officer (CRO) and the CMA has been designated as the agency's Senior Accountable Official (SAO) for risk management. Together the COO and CMA also chair the Management Control Oversight Council (MCOC), which provides the leadership and oversight necessary for effective implementation of NARA's Internal Control Program including ensuring risks are appropriately identified and managed. However, the two executives do not coordinate in an effort to effectively provide agency-wide oversight of cybersecurity risk activities, facilitate collaboration among stakeholders, and apply consistent application of a risk management strategies.

In accordance with *OMB Memorandum 17-25*, the CMA as the SAO is responsible for:

- implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data; and

- ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes, in accordance with chapter 35, subchapter II of title 44, United States Code.

Per OMB Memorandum 17-25, the SAO must have vision into all areas of the organization, particularly those focused on risk management; must possess authority for both funding and management of IT and enterprise risk; and must be able to represent the challenges and opportunities across the enterprise, we found NARA's SAOs responsibilities are not defined in NARA directives and the SAO only has responsibility over a portion of the agency.

Without clearly defining and documenting the responsibilities for the risk executive (function), NARA cannot ensure risk is managed consistently across the agency, organizational risk tolerances are appropriately reflected and considered along with other types of risk to ensure mission/business success.

Risk management strategy

NARA has not developed an enterprise-wide risk management strategy. NIST SP 800-39 indicates a risk management strategy makes explicit the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used within organizations for making investment and operational decisions. The risk management strategy also includes any strategic-level decisions and considerations on how senior leaders/executives are to manage information security risk to organizational operations and assets, individuals, other organizations, and the Nation.

NARA's Cybersecurity Framework Methodology (CFM) indicates the Office of Information Services has developed a comprehensive strategy to manage risk to NARA operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems. However, the comprehensive strategy defined within the CFM is a repeat of NIST guidance rather than an actual risk management strategy that serves as the foundation for managing risk and delineating the boundaries for risk-based decisions.

While NARA does not have an enterprise-wide risk tolerance used for making investment and operational decisions, Information Services' Chief Information Security Officer (CISO) and the Portfolio & Invest Services Delivery Office developed their own individual risk tolerances, neither of which were documented. For example, the CISO has an unofficial risk tolerance that requires system owners to remediate all critical or high weakness prior to an Authorization to

Operate being granted. The Portfolio & Invest Services Delivery Office gauges the overall health of a project by risk scoring (IT Health Checklist) the projects and programs (e.g., Share Drive Migration, eDocs Recompete, Windows 10/Office 16). Neither of these are a risk management strategy as required by NIST SP 800-39. Without an effective risk management strategy consistent with NIST guidelines, senior management may not be properly prepared to monitor, assess, and respond to risk.

Risk-based policies

NARA risk-based policies have not been fully documented or implemented. NIST SP 800-37, Revision 2 indicates elements of the risk-based policies include (1) identifying and assigning individuals with key roles for executing the risk management framework; (2) requiring an agency-wide assessment of cyber risks; (3) identifying and documenting common security controls that can be inherited by multiple information systems; (4) developing an agency-wide strategy for monitoring control effectiveness; (5) requiring system-level risk assessments to be performed and regularly updated; (6) tailoring system security controls based on risk; (7) prioritizing remedial actions to correct vulnerabilities identified in plans of action and milestones (POA&M) based on risk; and (8) using a determination of risk to make decisions about system operation and use.

The related NARA policies below do not accurately reflect individuals with key roles for executing the risk management framework.

- NARA directive 160, *NARA's Enterprise Governance, Risk, and Compliance (EGRC) Program* describes the major components of NARA's EGRC program, including NARA's Internal Control Program as defined in NARA 161.
- NARA directive 804, *Information Technology (IT) Systems Security* (April 2007), delineates the security management program structure, assigns responsibilities, and creates the foundation necessary to measure progress and compliance; and
- CFM records repeatable policies and processes used by NARA's Office of Information Services.

For example, although the CFM designated the COO as NARA's risk executive, the COO was unaware of these responsibilities. Additionally, NARA directives 160, 161, 804, and the CFM have not been updated to reflect the SAO or the October 2016 reorganization that includes the creation of the CMA role. Without accurately reflecting individuals with key roles for executing the risk management framework, NARA may not be able to properly facilitate risk-based decision making in managing cybersecurity risk.

Cybersecurity and enterprise risk management coordination

NARA has not established coordination between cybersecurity and enterprise risk management. Specifically, NARA has not implemented a capability for enterprise risk management in accordance with OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Currently, risk management responsibilities are performed by the (1) MCOC (ensures risks are appropriately identified and managed) (2) Chief Financial Officer (delegated the responsibility of ensuring compliance with OMB Circular A-123); (3) COO who serves as the CRO; and (4) SAO for risk management. However, the executives and MCOC have not created a process to share risks identified across the agency. For example, the CRO is not consistently made aware of information security risks identified by the Office of Information Services. While NARA's SAO is regularly briefed on these risks, the CRO is only briefed once or twice a year about the IT Security material weakness during the Executive Leadership Team and MCOC meetings.

NIST SP 800-39 states that effective risk management requires an agency's mission/business processes to explicitly account for information security risk when making operational decisions and that cybersecurity risk information should be shared with key stakeholders throughout the organization. The risk executive should serve as a common risk management resource for senior leaders, mission/business owners, and other organization officials; and as a focal point for communicating and sharing information security risk-related information among key stakeholders. Without an ERM program that includes effective cybersecurity and risk management coordination between the CRO, the CMA, and Information Services, NARA cannot effectively identify, assess, and prioritize actions to mitigate cybersecurity risks in the context of other enterprise risks. This in turn hampers the CRO's ability to make operational decisions to adequately address and mitigate risks.

Recommendations

We recommend:

Recommendation 1: The Chief of Management and Administration and the Chief Operating Officer ensure the Risk Executive, Chief of Management and Administration, Chief Operating Officer, and Senior Accountable Official for risk management roles and responsibilities are fully and accurately defined in NARA policies.

Management Response

NARA is currently revising NARA 160, NARA's Enterprise Governance, Risk, and Compliance Program, NARA 161, NARA's Internal Control Program, and NARA 804, Information Technology (IT) Systems Security, to address OIG recommendations from previous audits. NARA will ensure the revised policies clarify roles and responsibilities for risk management. Once those policies are updated, NARA will review NARA 101, NARA Organization and Delegation of Authority, and make additional changes to

functional statements and delegations if needed. This action plan requires an extended timeline to accommodate two rounds of policy formulation and review.

Target Completion Date: December 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of corrective actions identified above.

Recommendation 2: The Chief of Management and Administration develop, document, implement, and disseminate an organizational risk management strategy and policy, in accordance with NIST 800-39, and a process for coordination between cybersecurity and enterprise risk management.

Management Response

NARA is currently revising NARA 160, NARA's Enterprise Governance, Risk, and Compliance Program, NARA 161, NARA's Internal Control Program, and NARA 804, Information Technology (IT) Systems Security, to address OIG recommendations from previous audits. Once those policies are updated, NARA will develop a process for coordination between cybersecurity and risk management activities and functions. This action plan requires an extended timeline to accommodate two rounds of policy formulation and review.

Target Completion Date: December 31, 2021

OIG Analysis

We consider NARA's proposed actions responsive to our recommendation. This recommendation will remain open and resolved pending completion of corrective actions identified above.

Appendix A – Acronyms

Acronyms	Definition
CFM	Cybersecurity Framework Methodology
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Chief of Management and Administration
COO	Chief Operation Officer
CRO	Chief Risk Officer
EGRC	Enterprise Governance, Risk, and Compliance
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
ISSO	Information System Security Officer
IT	Information Technology
MCOC	Management Control Oversight Council
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMF	Risk Management Framework
SAO	Senior Accountable Official

Appendix B – Management Response

Date: August 25, 2020

To: James Springs, Inspector General

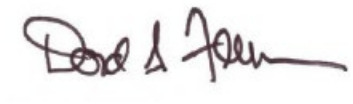
From: David S. Ferriero, Archivist of the United States

Subject: Action Plan to OIG Report 20-AUD-15, *Audit of NARA's Cybersecurity Risk Management Process*

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

We concur with the two recommendations in this audit and, in response, the attachment provides a summary of our proposed actions. We will provide documentation to your office as each recommendation is satisfied.

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

Action Plan Response to OIG Report 20-AUD-15,
Audit of NARA's Cybersecurity Risk Management Process

Recommendation 1: We recommend the Chief of Management and Administration and the Chief Operating Officer ensure the Risk Executive, Chief of Management and Administration, Chief Operating Officer, and Senior Accountable Official for risk management roles and responsibilities are fully and accurately defined in NARA policies.

Planned Action: NARA is currently revising NARA 160, NARA's Enterprise Governance, Risk, and Compliance Program, NARA 161, NARA's Internal Control Program, and NARA 804, Information Technology (IT) Systems Security, to address OIG recommendations from previous audits. NARA will ensure the revised policies clarify roles and responsibilities for risk management. Once those policies are updated, NARA will review NARA 101, NARA Organization and Delegation of Authority, and make additional changes to functional statements and delegations if needed. This action plan requires an extended timeline to accommodate two rounds of policy formulation and review.

Target Completion Date: December 31, 2021

Recommendation 2: We recommend the Chief of Management and Administration develop, document, implement, and disseminate an organizational risk management strategy and policy, in accordance with NIST 800-39, and a process for coordination between cybersecurity and enterprise risk management.

Planned Action: NARA is currently revising NARA 160, NARA's Enterprise Governance, Risk, and Compliance Program, NARA 161, NARA's Internal Control Program, and NARA 804, Information Technology (IT) Systems Security, to address OIG recommendations from previous audits. Once those policies are updated, NARA will develop a process for coordination between cybersecurity and risk management activities and functions. This action plan requires an extended timeline to accommodate two rounds of policy formulation and review.

Target Completion Date: December 31, 2021

Appendix C – Report Distribution List

Archivist of the United States
Deputy Archivist of the United States
Chief Operating Officer
Deputy Chief Operating Officer
Chief of Management and Administration
Chief Information Officer
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:
OIG Hotline
NARA
P.O. Box 1821
Hyattsville, MD 20788-0821