In Brief

Fiscal Year 2019 Independent Evaluation of the Smithsonian Institution's Information Security Program

OIG-A-20-06, September 30, 2020

What OIG Did

The Office of the Inspector General contracted with Williams Adley to conduct this audit. The audit objective was to evaluate the effectiveness of the Smithsonian's information security program in fiscal year 2019.

Background

Each year, the Department of Homeland Security and the Office of Management and Budget publish metrics to assist Inspectors General in their assessments of information security programs under the Federal Information Security Modernization Act.

The metrics rank the maturity level of five functions (Identify, Protect, Detect, Respond, and Recover) on a scale of 1 to 5. As an entity's information security program progresses in maturity, it moves from an informal ad hoc state (level 1) to formally documented policies and procedures (level 2) that are consistently implemented (level 3), managed through quantitative or qualitative measurement (level 4), and finally optimized based on mission needs (level 5).

When an entity achieves level 4 in at least three of the five cybersecurity functions, its information security program is considered effective overall.

What Was Found

For fiscal year 2019, Williams, Adley & Company - DC, LLP (Williams Adley) found that the Smithsonian Institution (Smithsonian) made improvements in its information security program, such as completing the implementation of the Information Security Continuous Monitoring (ISCM) strategy. ISCM helps to detect attempts that can damage information systems resulting in unauthorized access, data loss, operational failure, or unauthorized data modifications. However, further actions are needed in this area. For example, OCIO was not able to monitor and analyze security controls for 23 of 38 major information systems, and Williams Adley estimates it will take several years to complete the process for monitoring all 38 major systems. Until that process is complete, Williams Adley found that it will be difficult for the Smithsonian to monitor how well its information security program manages security risks.

In addition, the Office of the Chief Information Officer (OCIO) did not remediate high security vulnerabilities in a timely manner. OCIO managers said a new procedure was implemented in June 2019 to ensure vulnerabilities are addressed in a timely manner, but, because of the large backlog, remediations were not completed by the end of fiscal year 2019. Also, for two selected information systems (the Pan-Institutional Database for Advancement and a museum's collection information system), the system owners put data in these systems at risk because they did not periodically review user account activities to identify potential misuse of privileged user accounts. Furthermore, OCIO's inventory of the software components for these two selected systems was missing required information. Without fully understanding the complete software inventory, the system owners may not be adequately protecting critical software, which increases the risk to the information that resides on the software.

Overall, Williams Adley found that the Smithsonian's information security program was not effective. While the Detect function progressed to Level 3: Consistently Implemented in fiscal year 2019, the remaining four cybersecurity functions—Identity, Protect, Respond, and Recover—continued to operate at Level 2: Defined. For an information security program to be considered effective overall, at least three of the five cybersecurity functions must achieve Level 4.

What Was Recommended

Williams Adley made 17 recommendations to enhance information security at the Smithsonian. Management concurred with 15 recommendations and non-concurred with 2 recommendations.

For additional information or a copy of the full report, contact OIG at (202) 633-7050 or visit http://www.si.edu/oig.

OFFICE OF THE
INSPECTOR GENERAL

Smithsonian

Memo

Date: September 30, 2020

To: Lonnie Bunch, Secretary

Cc: Mike McCarthy, Undersecretary for Administration
Kevin Gover, Acting Undersecretary for Museum and Culture
Greg Bettwy, Chief of Staff, Office of the Secretary
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Deron Burba, Chief Information Officer
Carmen Iannacone, Chief Technology Officer, Office of the Chief Information Officer (OCIO)
Juliette Sheppard, Director, Information Technology Security, OCIO
Danee Gains Adams, Privacy Officer, OCIO
Robert J. Spiller, Assistant Secretary for Advancement
Zully Dorr, Deputy Assistant Secretary for Advancement
Machel Monenerkit, Acting Director, National Museum of the American Indian (NMAI)
Melanie Dann, Director, Advancement Operations and Systems, OA
Kara Lewis, System Owner, NMAI-Collections Information System
Erin Bordeaux, Assistant Director for Information Technology, NMAI
Stone Kelly, Program and Budget Analyst, Office of Planning, Management and Budget

From: Cathy L. Helm, Inspector General

Subject: *Fiscal Year 2019 Independent Evaluation of the Smithsonian Institution's Information Security Program* (OIG-A-20-06)

This memorandum transmits the final report of Williams, Adley & Company – DC, LLP (Williams Adley) on the fiscal year 2019 evaluation of the Smithsonian Institution's (Smithsonian) information security program.

Under a contract monitored by this office, the Office of the Inspector General engaged Williams Adley, an independent public accounting firm, to perform the audit. For fiscal year 2019, Williams Adley found that the Smithsonian has made improvements to its information security program but did not have an effective program as defined by the Department of Homeland Security. We made 17 recommendations for Smithsonian management to enhance information security at Smithsonian. Management concurred with 15 recommendations and did not concur with 2 recommendations. For the non-concurred recommendations, management

MRC 524
PO Box 37012
Washington DC 20013-7012
202.633.7050 Telephone
202.633.7079 Fax

disagreed that the system owners were responsible for maintaining specific inventory information. Management stated that certain inventory information is maintained by the Office of the Chief Information Officer in other various tools. OIG will follow-up with management to resolve this issue.

Williams Adley is responsible for the attached report and the conclusions expressed in the report. We reviewed Williams Adley's report and related documentation and interviewed their representatives. Our review disclosed no instances in which Williams Adley did not comply, in all material respects, with the U.S. Government Accountability Office's Government Auditing Standards.

We appreciate the courtesy and cooperation of all Smithsonian management and staff during this audit. If you have any questions, please call me or Joan Mockeridge, Assistant Inspector General for Audits, at (202) 633-7050.

Smithsonian Institution Office of the Inspector General

Report on the Smithsonian Institution's Information Security Program

Fiscal Year 2019

WILLIAMS ADLEY

CONTENTS

WILLIAMS ADLEY

Ms. Cathy Helm
Inspector General
Office of Inspector General
Smithsonian Institution
600 Maryland Ave, Suite 695E
Washington, DC 20024

Dear Ms. Helm:

We are pleased to provide our report for the performance audit we conducted to evaluate the effectiveness of the Smithsonian Institution's (SI) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year ending September 30, 2019.

FISMA requires each agency Inspector General, or an independent external auditor, to conduct an annual evaluation of their agency's information security program and practices, and to report to the Office of Management and Budget (OMB) on the results of their evaluations. OMB Memorandum M-19-02 (*"Memorandum for the Heads of Executive Departments and Agencies"*) provides instructions for meeting FY 2019 reporting requirements.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that 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 that evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Based on our audit procedures, we conclude that although SI has made improvements to its information security program and practices, SI continues to face challenges meeting the requirements of FISMA.

We have made recommendations related to the challenges faced by SI that, if effectively addressed by SI management, should strengthen the SI information security program. SI management has provided us with a response to this FY 2019 FISMA audit report. Their response is presented in its entirety in the Management's Response section of the report. We did not audit management's response and, accordingly, do not express any assurance on it.

This report is issued for the restricted use of the Office of Inspector General, the management of the SI, OMB, and the Department of Homeland Security.

Williams, Adley & Company-DC, LLP

September 29, 2020

WILLIAMS, ADLEY & COMPANY-DC, LLP
Management Consultants/Certified Public Accountants
1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161

INTRODUCTION

On behalf of the Office of the Inspector General (OIG), the auditing firm of Williams, Adley & Company-DC, LLP (Williams Adley) conducted an independent audit of the Smithsonian Institution's (SI) information security program and practices consistent with the Federal Information Security Modernization Act of 2014 (FISMA). SI is not required to comply with FISMA because SI is not an executive branch agency, but SI applies FISMA standards as a best practice to the extent practicable and consistent with its mission.

The fiscal year (FY) 2019 FISMA CyberScope metrics consist of five cybersecurity framework security functions: Identify, Protect, Detect, Respond, and Recover. These five functions comprise eight domains: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning. The Department of Homeland Security (DHS) uses the FISMA CyberScope metrics to determine the maturity of an entity's information security program. The maturity levels range from Level 1: Ad-hoc to Level 5: Optimized.

PURPOSE

FISMA requires the head of each executive branch agency to establish an entity-wide information security program that cost-effectively reduces information technology (IT) security risks to an acceptable level. To ensure the adequacy and effectiveness of the program, FISMA requires entity program officials, chief information officers, chief information security officers, senior entity official for privacy, and the OIG to conduct an annual reviews of the entity's information security program and to report the results to DHS.

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective was to conduct an independent audit of the effectiveness of SI's information security program and practices during the period October 1, 2018 through September 30, 2019 (FY2019).

SCOPE AND METHODOLOGY

An independent audit by Williams Adley of SI's IT security posture for programs and practices included testing the effectiveness of security controls for three (3) sampled SI systems. SI management assessed and categorized each of the three (3) systems as "Moderate" using the Standards for Security Categorization of Federal Information and Information Systems FIPS 199. SI does not currently have systems in the "High" category; thus, "Moderate" is the highest security category for systems in use at SI. Per FIPS 199, the unauthorized disclosure, modification, destruction, or disruption of access to a "Moderate" category system would have a serious adverse effect on SI's operations, assets, and stakeholders.

Williams Adley assessed the following three (3) SI systems:

- **Smithsonian Institution Network (SINet)**—SI's General Support System (GSS), which includes network transports, network security, and shared infrastructure, provides the core capability to the remainder of SI's major applications and miscellaneous IT systems.
- **Pan-Institutional Database for Advancement (PANDA)**—One (1) of SI's Moderate applications, which is the database of record for Smithsonian donations, contains the gift, pledge, matching gift, and membership transactions for the central Office of Advancement (OA) and the units. The system contains PII data that includes donors' contact information, such as address, email, and telephone number.
- **National Museum of the American Indian Collections Information System (NMAI-CIS)—**One (1) of SI's Moderate applications, which is used to manage assets the museum holds in trust for the Nation. NMAI-CIS currently provides a central repository for the Objects and Photographic Archives collections and holds approximately 5.6 terabytes (TB) of images for these collections.

The systems selected for testing are rotated annually among the 38 identified major IT systems and general support systems (GSS).

The SI OIG contracted Williams Adley to assess the effectiveness of SI's information security program and practices. Williams Adley performed the audit from June 2019 through October 2019, in accordance with Generally Accepted Government Auditing Standards (GAGAS). GAGAS requires Williams Adley to plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Williams Adley believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the review objectives.

In performing this audit, Williams Adley interviewed SI management and employees to evaluate the effectiveness of SI's information security program in accordance with SI, National Institute of Standards and Technology (NIST), and OMB guidance.

Williams Adley also observed daily operations, conducted sampling based on expert judgment where applicable, inspected SI policies and procedures to supplement observations and interviews, and obtained sufficient evidence to support the conclusions and recommendations. Where possible, Williams Adley also reviewed system-generated outputs to support the conclusions.

For the FY2019 Audit, Williams Adley used Inspector General (IG) FISMA CyberScope metrics to determine the status of SI's information security program. The FY2019 IG FISMA metrics consist of eight (8) domains, grouped into five (5) functional areas that correspond to the NIST Cybersecurity Framework. A list and description of the five functional areas and eight domains is presented in Appendix D. The metrics rank the organization's maturity level on a scale of 1 to 5 using 9–12 questions per level. See Table 1 (below) for a description of each level and see Appendix B for the detailed questions. Williams Adley's responses to each question were based on an assessment of both the entity-wide program and the three (3) systems selected for testing. To move from Level 1 to Level 2, the majority of the metrics must be Level 2 or greater, unless they are not applicable to the entity. For example, SI decided not to implement personal identity verification (PIV) cards and a Trusted Internet Connection (TIC); therefore, the fact that PIV and TIC were not implemented in the SI environment was not considered when determining the

maturity of SI's information security program. DHS considers an effective information security program to be Level 4: *Managed and Measurable*.

Table 1: Fiscal Year 2019 Maturity Model for FISMA Cybersecurity Functions

Level 5: Optimized Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.
Level 4: Managed and Measurable Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 3: Consistently Implemented Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 2: Defined Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 1: Ad-hoc Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.

Source: FY2019 IG FISMA Metrics

Note: In the context of the maturity models, Level 4 (Managed and Measurable) is considered an effective level by DHS. Generally, the Level 4 maturity level is defined as having formalized, documented, and consistently implemented policies, procedures, and strategies where quantitative and qualitative performance measures can be applied to determine the effectiveness of information security at the domain level, function level, and overall program level.

BACKGROUND

THE SMITHSONIAN INSTITUTION

SI was founded in 1846 with funds from the Englishman James Smithson (1765–1829) according to his wishes "under the name of the Smithsonian Institution, an establishment for the increase and diffusion of knowledge." SI, officially signed as a trust by President James K. Polk on August 10, 1846, was to be administered by a Board of Regents and a Secretary of SI.

SI, since its founding in 1846, has become the world's largest museum and research complex, consisting of 19 museums, the National Zoological Park, and nine (9) research facilities, libraries, and archives. A major portion of SI's operations is funded from annual federal appropriations. In addition to federal appropriations, SI receives private support, government grants and contracts,

and income from investments and various business activities. SI's federal funding for FY2019 is $1 billion, making SI 62% federally funded.

The Office of the Chief Information Officer

SI's OCIO plans and directs development, implementation, maintenance, enhancement, and operation of SI's information technology (IT) systems. In addition, the OCIO operates SI's computer facilities, equipment, web infrastructure, web-hosting services, telecommunications, and networks. The OCIO also provides management oversight of decentralized IT implementations by Smithsonian museums and units. The OCIO reports to SI's Undersecretary of Finance and Administration/Chief Operating Officer.

The OCIO has primary responsibility for setting IT security policy, managing SI's IT security program, and partnering with all units and system owners to evaluate IT system security for the 38 major IT systems. The IT security group is managed by the Director of IT Security, who reports directly to the Chief Information Officer (CIO). SI does not have any systems with a security categorization of "High," but does have systems with "Moderate" and "Low" security categorizations, as defined by Federal Information Processing Standards (FIPS) Publication 199.[1]

Smithsonian Privacy Office

The Smithsonian Privacy Office (SPO) works with units to minimize the collection of Personally Identifiable Information (PII) or personal information from any individuals, regardless of age or where or how collected, and to safeguard any information collected. The SPO also works with the units, including the Office of Contracting and Personal Property Management (OCon&PPM), the Office of Sponsored Projects (OSP), and the Office of General Counsel (OGC), to ensure that applicable privacy-related terms and conditions are included in contracts and agreements that involve the collection, use, storage, or dissemination of PII or sensitive personally identifiable information (sPII) by a third-party contractor. SPO also reviews and approves all collection, use, storage, and dissemination of PII and sPII at the unit level.

Federal Information Security Modernization Act of 2014

The Federal Information Security Modernization Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, was enacted to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Specifically, FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency. Also, each Inspector General (IG) is required to conduct an annual independent evaluation to determine the effectiveness of its agency's information security program and practices. The Office of Management and Budget (OMB) is required to ensure that guidance is developed for those evaluations.

Annually, OMB, in coordination with the United States Department of Homeland Security (DHS), provides guidance on reporting categories and responds to questions for meeting the current fiscal

[1] SI uses Federal Information Processing Standards Publication 199 to determine a system's security categorization.

year's reporting requirements.[2] OMB uses the data to carry out its oversight responsibilities and to prepare its annual report to Congress on the entities' compliance with FISMA. SI is not required to comply with FISMA because it is not an executive branch agency; however, SI applies FISMA standards as a best practice to the extent practicable and consistent with its mission. For details about FISMA domains and how they are scored, See Appendix D.

RESULTS OF AUDIT

OVERVIEW

Williams Adley assessed the effectiveness of SI's information security program and practices by reviewing documentation, meeting with SI and OCIO personnel, and performing onsite observations. Williams Adley determined that SI has developed policies, procedures, and strategies related to each IG FISMA metric domain. SI also has taken other explicit actions in each IG FISMA metric domain to improve its information security program. For example, SI created an information security architecture, updated policies and procedures in all functions, continued re-authorization of all SI information systems, and completed implementation of the ISCM strategy. SI's OCIO has several initiatives to continue improving its information security posture. However, SI is still in the process of authorizing or re-authorizing 23 of 38 major systems. One system that recently went through the re-authorization process did not have a configuration management plan.

As a result of this FISMA audit, Williams Adley encourages SI to continue to implement information security program processes in each IG FISMA domain, in accordance with NIST and OMB guidance.

IDENTIFY

The Identify function supports an understanding of the business context, the resources that support critical functions, and the related cybersecurity risks that enable an entity to focus and prioritize its efforts, consistent with its risk management strategy and business needs.[3] The Identify function is composed of the risk management process, which includes ongoing information system authorization, and promotes the concept of near-real-time risk management at the entity level, business process level, and information system level.

In FY2019, the Identify function operated at Level 2: Defined. SI was in the process of authorizing and re-authorizing most of the major systems; therefore, not all associated IT risks were centrally tracked using an automated governance, risk, and compliance (GRC) tool.

RISK MANAGEMENT

Risk management is the process of identifying, assessing, mitigating, and monitoring risks. An inconsistent and non-comprehensive risk management program creates an operating environment where information security risks could be overlooked and where mitigation strategies may not be

[2] OMB, *Fiscal Year 2018–2019 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-19-02, October 25, 2018.

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity version 1.1,* April 2018.

implemented. Without fully understanding the complete environment, management may be unknowingly accepting an unacceptable level of risk.

In FY2019, the risk management program operated at Level 2: Defined. SI improved its risk management program by (1) defining the importance and priority levels for its information systems to consider risks from the supporting business functions and mission impacts to guide risk management decisions; (2) defining and implementing the information security continuous monitoring strategy; (3) improving the risk management process by implementing a more robust communication of risks through meetings and workshops; (4) consistently implementing policies and procedures for plans of action and milestones (POA&M) maintenance, tracking, and review to ensure the POA&Ms have the information needed to be closed in accordance with SI's policies and procedures; (5) defining roles and responsibilities of stakeholders involved in risk management, and determining if these key individuals have been performing their roles and responsibilities as defined across the institution; (6) consistently implementing the defined policies and procedures that require specific security Federal Acquisition Regulation (FAR) clauses, and ensuring that specific contracting language and service-level agreements (SLA) are consistently included in contracts to mitigate and monitor the risks related to contractor systems and services; (7) consistently implementing the GRC tool to provide a centralized view of risks across SI's information systems; (8) and finalizing the Enterprise IT Security Architecture. SI also continued re-authorization efforts for all 38 major systems.

The re-authorization requirement was identified in the FY2014 report, which OIG closed in FY2018 with the understanding that OCIO would continue to complete re-authorization by implementing a planned schedule.[4] Part of this process includes determining if all identified major systems are, in fact, major systems, or if they should be reclassified as minor systems. However, by the end of FY2019, OCIO had not completed the re-authorization of SI's information systems.

Entity-level

(1) Not all information systems have completed re-authorization and are being tracked in the GRC tool.

NIST Special Publication (SP) 800-39*, Managing Information Security Risk; Organization, Mission, and Information System View*, March 2011, states: "organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation." The authorization process was first identified as an issue in the FY2014 report and re-authorization of all SI information systems was included in part of the response to the FY2014 recommendations. In FY2017, SI began implementing an automated GRC tool to provide a centralized view of risks across SI's information systems. By the end of FY2018, SI had completed the re-authorization process for six (6) major systems, which make up approximately 16% of the total re-authorization effort. SI completed the re-authorization of nine (9) major systems in 2019, bringing the current count to 15 of 38 systems (approximately 40%) operating with up-to-date authorization. However, by the end of FY2019, management was still in the process of re-authorizing the remaining 23 of 38 major systems. Until all systems are

[4] Clifton Larson Allen, *Fiscal Year 2014 Federal Information Security Management Act Independent Evaluation Report*, December 14, 2015.

re-authorized and the associated risks are entered into the automated GRC tool, SI may not be able to monitor how well its information security program is managing IT security risks.

System-level

(2) PANDA did not properly document all of its interconnections in its System Security Plan in FY2019.

OCIO's Information Technology Technical Standard & Guideline IT-930-03, *Security Assessment and Authorization Version 1.1*, Revision Date July 2019, requires all interconnections to be documented for each system. The System Security Plan (SSP) for each system, as well as the system inventory records for each system, must list all interconnections, whether or not the system is internal or external to the Smithsonian; however, Williams Adley determined that the interconnection, Enterprise Resource Planning (ERP) Financials, was not listed in the PANDA SSP in FY2019. After PANDA management was made aware of the missing interconnection, the ERP Financials interconnection was added to the SSP on October 15, 2019. Williams Adley will assess the newly updated SSP in FY2020. SI has developed system security policies to provide security measures to address the risks of unauthorized access or disruption of service; however, without complete SSPs, SI is at risk of transmitting and receiving financial reporting details without the necessary security controls in place to protect its systems and critical information.

PROTECT

The Protect function seeks to develop and implement safeguards to ensure the delivery of critical infrastructure services by supporting the ability to limit or contain the impact of a potential information security event. The Protect function comprises four (4) domains: configuration management, identity and access management, data protection and privacy, and security training.

In FY2019, the Protect function operated at maturity Level 2: Defined, which reflects the Protect function's four (4) domains. During FY2019, two (2) domains—configuration management and data protection and privacy—operated at Level 2: Defined. The identity and access management domain operated at Level 3: Consistently Implemented. The security training domain operated at Level 4: Managed and Measurable. The identity and access management domain and the security training domain have improved by one (1) maturity level since the FY2018 audit.

CONFIGURATION MANAGEMENT

Information systems continually change in response to updated hardware, new software capabilities, or patches to correct software flaws. Implementing such changes may require adjusting the system configuration. Configuration management is a collection of activities focused on establishing and maintaining the integrity of information systems by controlling the processes for initializing, changing, and monitoring the system configuration. Because changes may adversely affect an information system's security, a well-defined configuration management program must consider security implications when determining how to implement the changes.

In FY2019, the configuration management domain operated at Level 2: Defined. SI took steps to improve its configuration management program by ensuring that its baseline configuration and component inventory procedures are defined and dispersed. By the end of FY2019, SI had not addressed the following configuration management issues.

Entity-level

(1) OCIO did not update all of its configuration management policy documents within the defined timeframe.

OCIO's Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018, control CM-01, states that the configuration management policy and procedures should be reviewed and updated at least every 3 years. Williams Adley requested the current configuration management plan, policies, and procedures from OCIO. In response, OCIO provided Williams Adley with several technical notes[5] related to configuration management, but one (1) of the documents provided—Technical Note IT-960-TN01, *Change Management*—was last updated on August 8, 2013. In FY2019, per OCIO management, SI focused on finalizing the information security architecture and re-authorizing its information systems, leading to resource constraints for updating its configuration management plan. Without a comprehensive and up-to-date configuration management plan, SI could not efficiently support its configuration management processes. OCIO updated the manual on October 7, 2019. Williams Adley will assess the new update in FY2020.

(2) OCIO did not remediate High security vulnerabilities in a timely manner.

OCIO's Technical Note IT-930-TN33, *Vulnerability Management Program*, last revised August 29, 2019, defines the following remediation requirements based on asset criticality for Very High and High vulnerabilities:

- *High asset criticality – two (2) weeks to a month*
- *Very High asset criticality – five (5) days to a month*

Williams Adley conducted an aging analysis by comparing October 2018, March 2019, and June 2019 vulnerability scan reports for sampled Linux and Windows servers. Williams Adley determined that 161 of the Very High and High vulnerabilities for SINet Windows server and 100 Very High and High vulnerabilities for SINet Linux server were not remediated for more than eight (8) months. The Very High and High vulnerabilities that remain unresolved provide a readily available avenue for hackers. OCIO management personnel stated that a new procedure to ensure the vulnerabilities are addressed in a timely manner was implemented in June 2019, but, because of the large backlog, remediations were not completed by the end of FY2019.

System-level

(3) Two (2) of 22 completed and closed configuration changes were not approved by the Change Control Board (CCB) and nine (9) of 22 configuration changes in the SINet system did not have testing results documented as required.

OCIO's Technical Note IT-960-TN01, *Change Management*, August 8, 2013, states that for non-emergency changes, the CCB must approve the change ticket before the change is completed. In addition, if testing is completed, the testing process and the results must be documented. Williams Adley requested and inspected the supporting documentation for a sample of 22 changes and determined that two (2) of the 22 configuration changes had not been approved by the CCB, as required.

[5] In the SI environment, technical notes pertain to policies and procedures for operating and developing information technology as well as guidance on implementation.

In addition, test results were not documented for nine (9) of the 22 changes, as required. The change ticket assignees noted that testing had been completed, but did not include the associated testing results in the tracking system. Without proper approval of system changes, the CCB could not verify that the implementation of each planned change would be executed with minimum disruption to customers and other systems. If test results are not documented, then the CCB may be unable to verify that the change was implemented as approved and that no additional security impact resulted.

(4) SINet system owner did not maintain an accurate list of hardware inventory.

OCIO's Information Technology Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization Version 1.1,* Revision Date July 2019, states that the System Owner/System Owner Representative and Information Systems Security Officer (ISSO) are responsible for maintaining an inventory of all hardware, software, and other components that are included within their systems. System Owners/System Owner Representatives and ISSOs are responsible for ensuring that the information related to their systems remains current.

OCIO provided Williams Adley with the official hardware component inventory list for its data center, and Williams Adley conducted two (2) tests to verify that the inventory was accurate and complete. For the first test, Williams Adley selected 12 servers from the inventory and attempted to physically locate them at the data center; Williams Adley determined that the current location of one (1) of the 12 servers was not accurately documented. OCIO staff stated that Smithsonian Enterprise (SE) personnel had relocated the server without informing OCIO of the move; therefore, the location of the inventory had not been updated in the tracking system. For the second test, Williams Adley selected 13 servers from the data center and traced them back to the component system inventory and determined that one (1) of 13 decommissioned servers was still noted as "Active" and "Operational" in its record and operation status. OCIO stated there is a lag time between when the change is performed and when the documentation is. Without fully understanding the complete hardware inventory, including where devices are physically located, management may be hampered in responding to time-sensitive security issues.

(5) Roles and responsibilities were not fully defined in the PANDA system's configuration management policies and procedures.

OCIO's Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2,* Revision Date August 2018*,* states that control CM-09 is required; however, because the associated language detail was not provided in IT-930-02, Williams Adley used the supporting NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013, control CM-09, which states, "the organization develops, documents, and implements a configuration management plan for the information system that: (1) addresses roles, responsibilities, and configuration management processes and procedures; (2) establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; (3) defines the configuration items for the information system and places the configuration items under configuration management; and (4) protects the configuration management plan from unauthorized disclosure and modification."

PANDA personnel provided Williams Adley with the PANDA system's configuration management policies and procedures document. Williams Adley determined that the document

did not define the responsibilities of configuration management personnel as required, despite the fact that PANDA had just gone through the re-authorization steps in FY2018, one of which was to ensure that policies and procedures contain all required information. Without identifying the responsibilities for configuration management personnel, there would be a lack of accountability for progressing through the configuration management processes.

(6) NMAI-CIS's system owner did not consistently implement the requirement to have defined system-level configuration management procedures.

According to NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, control CM-1, "the organization develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance." Williams Adley requested the configuration management policies and procedures for NMAI-CIS to determine if there is a defined process for managing configuration changes. Williams Adley determined that although NMAI-CIS manages configuration and operational tasks using the Jira ticketing system, there are no formal policies or procedures for the change request process for Electronic Museum Collection (EMu) application. As NMAI-CIS transitioned through the ATO process, the fact that the system did not have a configuration management procedure was not identified. Without establishing a defined system-level configuration management procedure, NMAI management may not effectively develop, approve, or implement configuration changes.

(7) Two (2) of two (2) selected information system software component inventory lists did not include appropriate inventory details per SI's taxonomy requirement.

OCIO's Information Technology Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization Version 1.1,* Revision Date July 2019, states that "on an annual basis, Information Technology System Security (ITSS) will ask System Owners and Smithsonian Unit IT Managers to review the inventory of IT systems and provide any changes; System Owners/System Owner Representatives and ISSOs will review and update the component inventories for their systems at least annually."

In addition, NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Updated January 22, 2015, control CM-8, states that "the organization develops and documents an inventory of information system components that is at the level of granularity deemed necessary for tracking and reporting; and includes organization-defined information deemed necessary to achieve effective information system component accountability. Organizations may choose to implement centralized system component inventories that include components from all organizational systems. In such situations, organizations ensure that the inventories include system-specific information required for proper component accountability. Information necessary for effective accountability of system components includes, for example, hardware inventory specifications; software license information; software component owners; version numbers; and for networked components or devices, the machine names and network

addresses. Inventory specifications include, for example, manufacturer; device type; model; serial number; and physical location."

SI's taxonomy document requires inclusion of the device name, Internet Protocol (IP) address, location, image name, software version, system contact, product type, last boot time, image type, image family, and serial number for hardware and software assets.

For PANDA, Williams Adley noted that only the names and descriptions of the servers were tracked, along with the associated software on the PANDA inventory list. The list did not provide a location, asset number, or owner, all of which are required to be included in a full hardware and software component inventory. These additional details should be maintained by the various tools (e.g., Casper, System Center Configuration Manager (SCCM)) and units (e.g., OCIO, System Owners, SE) found throughout SI; however, the details were not provided during the audit. OCIO stated that the hardware and software information is gathered, but not all information is maintained in in one location.

For NMAI-CIS, Williams Adley was provided with the NMAI-CIS list of hardware and software component inventories, and determined that the hardware inventory list did not provide a location, asset number, or owner. These additional details should be maintained by various tools (e.g., Casper, SCCM) and units (e.g., OCIO, System Owners, SE) found throughout SI; however, the details were not provided during the audit. OCIO stated that the hardware and software information is gathered, but not all information is maintained in one location.

Without fully understanding the complete software inventory, system owners may not be adequately protecting critical software, which increases the risk to the information that resides on the software.

(8) PANDA did not properly manage configuration changes in accordance with the system's Operations Guide.

According to the *PANDA Operations Guide*, dated August 26, 2019, the approved signature of the Director of Advancement Information System (AIS) is needed for system changes before the changes are made. Williams Adley requested the supporting documentation for eight (8) of 75 application changes. After reviewing the supporting documents, Williams Adley determined that five (5) of eight (8) changes were not approved before the specifications were assigned to coders and testers. PANDA management stated that there was an undocumented process where the final signature for specification is obtained after the changes are deployed; however, Williams Adley determined that such undocumented procedures were not consistently followed for all changes. The PANDA management team is expected to update the PANDA Operations Guide to reflect the undocumented process in FY2020.

Identity and Access Management

Effective access control processes are critical to prevent unauthorized dissemination or modification of data because they ensure that only approved and authorized personnel have access to SI information. Lack of an effective identity and access management practice increases the risk of unauthorized system access, whether by internal employees or external attackers, endangering the confidentiality, integrity, and availability of SI systems.

In FY2019, the identity and access management process operated at Level 3: Consistently Implemented. The identity and access management process progressed from maturity Level 2:

Defined in FY2018 because OCIO made progress by implementing two-factor authentication for enterprise administrators and ensuring the defined roles and responsibilities for identity and access management are carried out throughout the institution. However, access agreements for individuals who can access the Smithsonian network were not properly maintained, privileged user account activities were not reviewed on a system level, and not all identity and access management policies and procedures were up to date throughout FY2019.

Entity-level

(1) OCIO did not update all of its identity and access management policy documents within the defined timeframe.

OCIO's Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018, control AC-01, states that the "identity and access management policy and procedures should be reviewed and updated at least every three (3) years." Williams Adley requested the current identity and access management policy and procedures from OCIO, and OCIO provided Williams Adley with several technical notes[6] surrounding identity and access management; however, one (1) of the technical notes provided—Technical Note IT-930-TN37, *Securing IT Accounts*—had not been updated for four (4) years since its initial release in October 2015, although a review is required at least every three (3) years. IT-930-TN37 also specified the need for passwords, length, and complexity, but did not detail the required use of two-factor authentication for privileged users. In FY2019, per OCIO management, SI focused on updating the technical notes with more critical changes. Without comprehensive and up-to-date identity and access management policies and procedures, SI cannot efficiently support its identity and access management processes because the defined authentication requirements for privileged users were outdated.

(2) OCIO did not implement the NIST-recommended two-factor authentication for all identified privileged users who access its network.

NIST SP 800-63B *Digital Identity Guidelines*, June 2017, states that stronger authentication requires malicious actors to have better capabilities and to expend more resources to successfully subvert the authentication process. Authentication at higher levels can effectively reduce the risk of attacks. A password-only system is vulnerable because users tend to use the same password across multiple systems and because users are targets of phishing and social engineering attacks. Adding a second factor, such as a physical security token, is a stronger authentication method than a simple password.

Williams Adley's review found that OCIO has implemented strong authentication—Entrust security token—for all users for remote access, and for privileged users who are Tier 0. SI has planned for, but not implemented, the use of strong authentication mechanisms for other privileged users to access its systems and network before the end of the year as resources were focused on other priorities. Without strong authentication, less sophisticated cyber criminals or insiders could gain unauthorized access to SI's information and systems.

[6] In the SI environment, technical notes pertain to policies and procedures for operating and developing information technology as well as guidance on implementation.

(3) OCIO does not have defined policies and procedures for reviewing audit logs, which includes a list of defined auditable events or activities by remote users using a Virtual Private Network (VPN) or Citrix.

NIST SPSP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, states that the organization should provide organization-defined information system monitoring information to personnel. Williams Adley requested the current policies and procedures for the review of audit logs, including a list of defined auditable events and a list of activities by remote users using VPN or Citrix. OCIO management stated that although SI does not have the required policies and procedures defined, VPN and Citrix logs are sent to the Security Information and Event Management unit, which has alerts that cover remote access activities. Without fully defined and implemented incident monitoring policies and procedures, SI may be unable to detect malicious events in a timely manner.

(4) One (1) sampled NMAI-CIS privileged user did not sign an elevated privileges agreement or complete the privileged user security training before gaining privileged access, as required.

OCIO Technical Note IT-930-TN37, *Securing IT Accounts*, October 30, 2015, states that all privileged users must sign an Elevated Privileges Agreement before receiving administrative credentials. Personnel with administrative privileges to any IT system also must complete course S-111: Privileged User Security and sign an Elevated Privileges Agreement.

Williams Adley selected one (1) NMAI-CIS privileged user account in FY2019 for testing. Williams Adley determined that the NMAI-CIS privileged user (NMAI-CIS Administrator) did not take the required Privileged User Security Training (S-111) within 30 days of gaining access to NMAI-CIS and did not sign an Elevated Privileges Agreement form. The S-111 training was not completed until 160 days after completion. The privileged user had been with NMAI-CIS on a part time basis before the privileged user agreement and training requirements were in place and NMAI-CIS did not initially understand that the form was required for users currently in place. Without proper security training, the privileged user may lack the IT security awareness needed to recognize threats and to make decisions that reduce risk. Without reading and signing the Privileged User Agreement, the privileged user may not understand the responsibilities of a privileged user, the acceptable rules of behavior, or the importance of the role with which the user is entrusted.

(5) PANDA and NMAI-CIS system owners did not periodically review user account activities for misuse, as required by OCIO policy. In addition, SI did not define policies and procedures for reviewing user account activities, aside from dormant accounts.

OCIO Technical Note IT-930-TN37, *Securing IT Accounts*, October 30, 2015, specifies that each system must have a documented process for managing accounts that includes: a process to periodically review accounts at least quarterly and to modify or deactivate accounts as appropriate.

Williams Adley requested copies of the current policies and procedures for reviewing user account activities, such as privileged user activities, from PANDA and NMAI-CIS. PANDA and NMAI-CIS system owners provided only the policies and procedures for reviewing dormant accounts. Williams Adley requested supporting evidence indicating that periodic reviews from PANDA and NMAI-CIS were conducted and documented, but PANDA and NMAI-CIS management could

only provide supporting documentation for the review of dormant accounts. During Williams Adley's inquiries with PANDA and NMAI-CIS management about their process for quarterly reviews, PANDA and NMAI-CIS management stated that although they periodically review privileged user activities, there was documentation only for the dormant account reviews. Without defined policies and procedures for reviewing user account activities, PANDA and NMAI-CIS system owners could not properly protect their data by identifying user behavior that might indicate privilege abuse or violation of the Privileged User Agreement. Also, if there is no proper logging or periodic review of user account activity, a misuse of privileged functions may not be detected.

Data Protection and Privacy

Sensitive information, including PII and sPII, should be protected from inappropriate dissemination. Data Protection and Privacy (DPP) is about preventing the unwanted release of sensitive information and responding to any instances where information is found to be inadvertently shared.

In FY2019, DPP operated at Level 2: Defined. Williams Adley noted that the SPO has made progress in reducing the number of PII holdings and in identifying all systems that require a privacy assessment; has ensured that privacy awareness training is provided to all individuals; and has initiated periodic privacy reviews of IT systems. In addition, SI has enhanced its network defense. However, there remain areas for improvement, such as continuing to update policy and procedures, implementing more privacy training for all staff across the organization, and ensuring that privacy assessments are completed for all information systems.

Entity-level

(1) The Privacy Office did not maintain up-to-date privacy policies and procedures throughout FY2019.

Smithsonian Directive (SD) 118 *Privacy Policy*, March 11, 2014, states that SD 118 must be reviewed at least every two (2) years. SD 119, *Privacy Breach Policy*, September 12, 2018, also states that the policy must be reviewed annually. The SPO's privacy program has a defined program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems. However, not all privacy policies and procedures were up to date throughout FY2019. Specifically, SD 118, *Privacy Policy* had not been updated since it was first finalized on March 11, 2014.

According to the Smithsonian Privacy Officer, SD 118 is in the process of being updated, but the update was not completed in FY2019 because the majority of efforts were focused on conducting a PII inventory of all information systems in use. Furthermore, the updated SD 119 provides more critical information than SD 118, and SPO has conflicting guidance in SD 118 and SD 119. Because SPO has not updated SD 118, users might fail to comply with the new laws and regulations as updated in SD 119. If SPO's policies on adequate data protection and privacy awareness (e.g., what is considered a PII violation) are not consistent, PII could be mismanaged and improperly handled by stakeholders who rely on them for compliance guidance.

(2) OCIO did not implement the data loss prevention function in Microsoft Office 365 across SI.

OCIO's Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018, Control Number SI-04(4), states, "the information system monitors inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions." Williams Adley inquired with OCIO to determine if SI had implemented data loss protection tools to monitor data for leakage of sensitive information.

Williams Adley determined that OCIO had implemented the Data Loss Prevention (DLP) function in Microsoft Office 365 for the Human Resources (HR) unit to prevent data loss, but that the DLP policy for function alerts to OCIO personnel of potential leakage of sensitive information for all other SI units was violated. Although SI scans outgoing emails for potential sensitive information, without a DLP tool in place to proactively alert all users before the leakage of sensitive information, OCIO would be unable to fully prevent sensitive information from being intentionally or unintentionally shared with outside parties if it was implemented only for the HR unit and not for all other SI units. OCIO stated that SI has plans to implement additional DLP capabilities and that there is an open IG recommendation for its implementation.

(3) OCIO has not consistently implemented the security controls for encryption of data in transit to protect its PII and other agency-sensitive data, as appropriate, throughout the data lifecycle.

OCIO Technical Note IT-930-TN23, *Electronic Authentication*, Revision Date March 29, 2017, requires the information system to implement cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to data during transmission. It states that the highest available level of Transport Layer Security (TLS) should be used. Renegotiation down to the less secure Secure Sockets Layer (SSL) or TLS 1.0 protocols is not allowed. All Smithsonian systems using SSL or TLS must upgrade to TLS 1.2 by June 30, 2017.

Williams Adley determined that although encryption was in place for transmitting sensitive information, many systems were using vulnerable SSL and TLS versions. OCIO was in the process of migrating all systems to TLS 1.2. OCIO management stated that SI was also migrating from Windows 7 to Windows 10 and expected the migration to be completed in the beginning of FY2020. Without implementing the security controls for encryption of data in transit, PII and other agency-sensitive data can be obtained by unauthorized personnel, leading to damage to the entity's reputation and/or to financial loss.

(4) The Privacy Office has not conducted DPP-specific tabletop exercises, or developed any lessons learned in FY2019.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Updated January 22, 2015, states that the organization should "develop and implement a Privacy Incident Response Plan; and provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan." NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, states that the development of response plans for breaches involving PII requires organizations to make decisions about how to handle breaches involving PII, that the decisions

should be used to develop policies and procedures, and that the policies and procedures should be communicated to the organization's entire staff through training and awareness programs. Training may include tabletop exercises to simulate an incident and to test whether or not the response plan is effective and whether or not staff members understand and are able to perform their roles effectively. Training programs should also inform employees of the consequences inappropriate use or handling of PII.

Williams Adley was informed by the SPO that SI had not conducted a DPP-specific tabletop exercise or developed lessons learned in FY2019. This was primarily because SPO had prioritized their efforts into the completion of privacy assessments for required SI information systems. Lessons learned should be captured at the end of any tabletop exercise or incident; however, no incident was closed during FY2019. Without conducting tabletop exercises or developing lessons learned, the SPO may be unable to make improvements to the plan, as appropriate.

Security Training

People are often the weakest link in security. Security training helps to ensure that personnel at all levels understand their information security responsibilities to properly use and protect the information and the resources entrusted to them. Therefore, a well-defined security training process must include continual training of the workforce on organizational security policy and role-based security responsibilities to increase its rate of success in protecting information.

In FY2019, the Security Training program operated at Level 4: Managed and Measurable. OCIO improved the security training domain by tailoring its annual security awareness training and by conducting internal reviews of all training annually to determine its appropriateness. OCIO also consistently implemented its organization-wide security awareness and training strategy and plan. In addition, SI allocated sufficient resources to consistently carry out its security awareness and training responsibilities, including an IT training budget for enterprise-wide Computer Security Awareness Training (CSAT) as well as role-based training. OCIO also conducted an informal skill gap assessment in FY2019; however, Williams Adley noted that SI has not defined policies and procedures for assessing the knowledge, skills, and abilities of SI's workforce and, specifically, for gap remediation.

Entity-level

(1) OCIO did not conduct a formal skill assessment for SI's workforce.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003,[7] recommends that a high-level security training strategy include the following components: structure of the awareness and training program, priorities, funding, goals of the program, target audiences, types of courses and material for each audience, and use of technologies. NIST SP 800-50 further states that "completion of the needs-assessment allows an agency to develop a strategy for developing, implementing, and maintaining its IT security awareness and training program." Williams Adley noted that OCIO did not conduct a formal skill assessment within all functional areas; however, OCIO did perform an informal skill gap assessment in FY2019 and documented the results in its *SI Enterprise IT Security Architecture* document. Williams Adley also noted that SI has not defined policies and procedures for assessing the knowledge, skills, and abilities of SI's workforce or, specifically, for gap remediation. OCIO

[7] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

management stated that OCIO tracks security trends and updates general security awareness training annually with input from individuals throughout SI. Without a formal skill assessment, OCIO may be unable to effectively target its limited training resources on the most important security knowledge gaps.

DETECT

The Detect function of the Cybersecurity Framework enables timely discovery of an information security event. The Detect function comprises one (1) domain—Information Security Continuous Monitoring (ISCM)—which seeks to provide visibility into IT assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls.

In FY2019, the Detect function operated at Level 3: Consistently Implemented. SI made progress toward completing the ISCM program phases to implement its ISCM strategy and is in the continuous improvement stage. However, some areas of the ISCM program could be improved at the system level.

INFORMATION SECURITY CONTINUOUS MONITORING

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[8] Without a fully implemented ISCM program, OCIO may be unable to detect attempts to damage its systems, resulting in unauthorized access, data loss, operational failure, or unauthorized data modification. OCIO also would be unable to develop the key security metrics needed to measure and monitor the effectiveness of its current information security posture.[9]

In FY2019, ISCM operated at Level 3: Consistently Implemented. OCIO improved the Detect function by consistently implementing lessons learned, and consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program. All the tools and architecture specified in the ISCM strategy were in place and OCIO added several new monitoring tools in FY2019. By the end of FY2019, more than 150 alerts had been created in Splunk, and OCIO planned to continually add new alerts based on risk assessments. System-specific dashboards are used to coordinate threats using the alerts created in Splunk; however, Williams Adley noted that although OCIO identified dashboards in its strategy, OCIO did not provide system-specific dashboards across the enterprise for monitoring correlated threats, including the 150 alerts created in Splunk, at the system level.

Entity-level

(1) OCIO is not able to monitor and analyze security controls for 23 of 38 major information systems.

According to NIST SP 800-137, *ISCM for Federal Information Systems and Organizations,* September 2011, an effective ISCM begins with development of a strategy that addresses ISCM requirements and activities at each organizational tier (organization, mission/business processes,

[8] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011.

[9] Security posture includes the design and implementation of security plans and the approach the entity takes to information security. It comprises technical and non-technical policies, procedures, and controls to protect the entity from internal and external threats.

and information systems). Each tier monitors security metrics and assesses security controls' effectiveness with established monitoring and assessment frequencies and status reports customized to support tier-specific decision-making.

Smithsonian ISCM requirements are documented using an ATO process through the Archer system. However, security controls, their effectiveness, their metrics, and their assessment frequencies were not monitored completely for 23 of 38 systems; only 15 systems had completed the ATO process through the Archer System. OCIO has been working to ATO all identified major systems, however, as this process can take months to complete, it will take several years to get through all 38 systems. Without monitoring all security controls, critical metrics, and risks, there may be gaps in the security of the remaining 23 information systems.

RESPOND

The Respond function, which consists of incident response, supports the ability to take action in response to a detected cybersecurity incident and to limit the incident's impact. As stated in OCIO Technical Note IT-930-TN30, *IT Security Incident Response Plan and Procedures*, information systems are subject to a range of security incidents that can have a serious impact on SI's ability to perform its mission.

In FY2019, the Respond function operated at Level 2: Defined. OCIO made several improvements in the Incident Response program; however, there are areas that can still be improved, such as reporting incidents to external stakeholders in a timely manner.

INCIDENT RESPONSE

OCIO Technical Note IT-930-TN30, *IT Security Incident Response Plan and Procedures*, states that incident response is important for rapidly detecting, limiting the effects of, and recovering from IT security incidents. An incident response capability is essential for minimizing loss and restoring computer services in a timely manner. A response also includes assessing the types of attacks that have been successful and using that information to make risk-based decisions.

In FY2019, SI's incident response program operated at Level 2: Defined. Improvements during FY2019 included OCIO implementation of email anti-malware and host-based anti-malware tools to support incident response activities. In addition, OCIO implemented a program to automatically report security incidents to internal and external stakeholders. There are areas, however, that can be improved, such as reporting incidents to external stakeholders in a timely manner.

Entity-level

(1) OCIO did not categorize security incidents with impact levels in a timely manner.

OCIO Technical Note IT-930-TN30, *IT Security Incident Response Plan and Procedures*, requires all IT security incidents to be documented with appropriate categorization. Williams Adley tested a sample of four (4) identified security incidents in FY2019 and verified that three (3) had not been categorized initially. The Security Operations Center (SOC) lead stated that the three (3) security incidents were not categorized with the proper impact levels in a timely manner due to an error made by SOC staff; therefore, the proper impact-level assignment was delayed. The delay in categorizing security incidents with impact levels delayed OCIO's ability to notify all internal and external stakeholders in a timely manner as required.

RECOVER

The Recover function seeks to reduce the negative impact of an information security event through the timely recovery of normal operations via contingency planning.

In FY2019, the Recover function operated at Level 2: Defined. OCIO made progress in consistently implementing roles and responsibilities of contingency planning stakeholders, updated and implemented an entity-wide IT Disaster Recovery Plan (DRP) document, and conducted an entity-level business impact analysis (BIA) in FY2019. However, some areas of the contingency planning program could be improved at the system level.

CONTINGENCY PLANNING

OCIO Information Technology Technical Standards & Guidelines IT-960-02, *IT Disaster Recovery Planning*, states that the contingency planning program should provide management with policies and procedures to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters. Disaster recovery is a type of contingency plan for recovering one (1) or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

In FY2019, SI's contingency planning program operated at Level 2: Defined. Improvements during FY2019 included OCIO finalizing a defined process for conducting a BIA and beginning to conduct an enterprise-wide BIA using Archer to guide contingency planning efforts. OCIO also finalized a DRP for critical systems housed in the data center, which includes defined roles and responsibilities and communication processes. However, there are areas that can be improved, such as ensuring that each system owner uses the results of a system-specific BIA for DR planning and conducting annual contingency plan testing.

System-level

(1) NMAI-CIS system owner did not perform an annual contingency plan test in FY2019.

According to NMAI-CIS *System Security Plan*, the NMAI-CIS team tests the contingency plan for the NMAI-CIS annually using tabletop exercises to determine the effectiveness of the plan and the organization's readiness to execute the plan.

Williams Adley requested NMAI-CIS incident response testing information and was informed by NMAI-CIS personnel that system-level contingency plan testing in FY2019 was not completed. The system owner prioritized the completion of the ATO and thus had insufficient time in FY 2019 to test the contingency plan. The testing was performed in the fall of 2019. Not performing contingency plan testing would mean that NMAI-CIS personnel would be unable to evaluate the effectiveness of their contingency plan and their readiness to execute the plan or to leverage crucial information from the testing to enhance their contingency plan processes.

(2) PANDA and NMAI-CIS system owners did not develop a system-level Business Impact Analysis (BIA) (e.g., calculation for the system's recovery criticality) for their systems.

OCIO Information Technology Technical Standards & Guidelines IT-960-02, *IT Disaster Recovery Planning*, requires the DR coordinator for the system to analyze the supported mission and business processes and to work with process owners and business managers to determine the

acceptable downtime if a given process or if specific system data were disrupted or otherwise unavailable. This includes defining the Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO). It also states that the estimated downtime should be included in the BIA, which includes MTD, RTO, and RPO.

Williams Adley requested and reviewed PANDA and NMAI-CIS contingency plans and determined that the contingency plans were developed without system-level BIAs that contain details on MTD, RTO, or RPO. Without first completing and documenting the system-level BIAs, PANDA and NMAI-CIS contingency plans may be unable to recover the most critical assets within a reasonable timeframe. As a result, the plans may not be adequate to allow SI to recover from a disaster in the most effective and efficient manner. PANDA and NMAI-CIS system owners indicated that they will consider developing and performing BIAs and will include the MTD, RTO, and RPO in future contingency plans.

CONCLUSION

Based on Williams Adley's independent audit of the Smithsonian Institution's information security posture for programs and practices and consistent with the Federal Information Security Modernization Act of 2014 (FISMA), Williams Adley determined that while the Smithsonian Institution has made improvements across several domains, it did not achieve the information security goals identified by DHS, which is Level 4: Managed and Measurable. Williams Adley makes the following recommendations to help Smithsonian Institution enhance its information security program

RECOMMENDATIONS

To improve SI's information security program, Williams Adley makes the following recommendations to the Chief Information Officer:

Recommendation 1: Perform timely reviews and update policies and procedures at the required frequency, in accordance with IT-930-02, *Security Controls Manual, Version 4.2* for IT-930-TN37, *Securing IT Accounts* and SD 118*, Privacy Policy*.

Recommendation 2: Remediate vulnerabilities in the OCIO-defined timely manner.

Recommendation 3: Develop a process to review change tickets to verify that all system changes are documented, approved, and tested before migrating the changes to production.

Recommendation 4: Develop a process to verify that all incidents are properly categorized to ensure all security incidents are reported in a timely manner.

Recommendation 5: Develop and conduct privacy-specific tabletop exercises and capture lessons learned.

Recommendation 6: Upgrade all Smithsonian systems currently using Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TLS 1.2.

Williams Adley makes the following recommendations to the PANDA system owner:

R**ecommendation 7:** Develop a procedure to identify and document system interconnections in the PANDA System Security Plan.

Recommendation 8: Implement a review process to ensure that all system-specific change specifications are approved before they are migrated to the production environment.

Recommendation 9: Define roles and responsibilities for key stakeholders in the PANDA system's configuration management policies and procedure.

Recommendation 10: Develop a process to ensure user account activities, and associated audit logs, are reviewed and documented by the PANDA system owner as required by OCIO Technical Note IT-930-TN37, *Securing IT Accounts.*

Recommendation 11: Document and maintain detailed software and hardware inventory lists for the PANDA system consistent with SI policies and procedures.

Recommendation 12: Conduct and document a system-level BIA that identifies the maximum tolerable downtime (MTD), recovery time objectives (RTO), and recovery point objectives (RPO), and document the MTD, RPO, and RTO in the contingency plans.

Williams Adley makes the following recommendations to the NMAI-CIS system owner:

Recommendation 13: Test and update the NMAI-CIS system contingency plan annually.

Recommendation 14: Develop and implement NMAI-CIS system-level configuration management policies and procedures.

Recommendation 15: Develop a process to ensure user account activities, and associated audit logs, are reviewed and documented by the NMAI-CIS system owner as required by OCIO Technical Note IT-930-TN37, *Securing IT Accounts.*

Recommendation 16: Document and maintain a detailed software and hardware inventory list for the NMAI-CIS system that is consistent with SI policies and procedures.

Recommendation 17: Conduct and document a system-level BIA that identifies the maximum tolerable downtime (MTD), recovery time objectives (RTO), and recovery point objectives (RPO), and document the MTD, RPO, and RTO in the contingency plans.

MANAGEMENT'S COMMENTS AND WILLIAMS ADLEY'S RESPONSE

OIG provided the Smithsonian a draft of Williams Adley's report for review and comment, and Smithsonian management provided written comments. In the written comments, which are reproduced in their entirety in Appendix F, management concurred with 15 recommendations and outlined actions planned to address them. Management did not concur with 2 recommendations, 11 and 16 that required Panda and NMAI-CIS system owners, respectively to document and maintain a detailed software and hardware inventory that is consistent with SI policies and procedures. According to OCIO, both system owners were compliant with SI inventory procedures for their systems and OCIO specified that additional information is maintained centrally in other tools that are managed by OCIO. Williams Adley made this point in the report. Nevertheless, OCIO has not provided any evidence that complete hardware and software inventory information is gathered and maintained by other tools.

APPENDIX A – CRITERIA

The following National Institute of Standards and Technology (NIST) guidance, federal standards, and Smithsonian Institution (SI) policies were used to evaluate SI's information security program.

Office of Management and Budget (OMB) Memorandum (M)-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018.

Risk Management

a. NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and System View,* March 2011
b. NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations,* December 2018
c. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013
d. NIST SP 800-60 Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
e. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Security Systems,* February 2004
f. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018
g. SI Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization Version 1.1,* Revision Date July 2019

Configuration Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018
b. SI Technical Note IT-930-TN33, *Vulnerability Management Program*, last revised August 29, 2019
c. SI Technical Note IT-960-TN01, *Change Management*, August 08, 2013
d. SI Technical Note IT-920-TN04, *Configuration Management*, March 29, 2019
e. *PANDA Operations Guide*, August 26, 2019
f. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Updated January 22, 2015

Identity and Access Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018
b. SI Technical Note IT-930-TN37, *Securing IT Accounts,* October 30, 2015
c. NIST SP 800-63B, *Digital Identity Guidelines*, Updated June 1, 2017
d. *Pan-Institutional Database for Advancement User Access Protocol*, Version 11.0, Revision Date July 3, 2019
e. *NMAI-CIS User Account Creation, Renewal, and Disabling Processes*, Updated August 26, 2019

Data Protection and Privacy

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018
b. Smithsonian Directive 118, *Privacy Policy*, March 11, 2014
c. Smithsonian Directive 119, *Privacy Breach Policy*, September 12, 2018
d. SI Technical Note IT-930-TN23, *Electronic Authorization,* March 29, 2017
e. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010

Security Training

a. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003

Information Security Continuous Monitoring

a. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011
b. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, Revision Date August 2018
c. SI Information Technology Technical Standards & Guidelines IT-930-03, *Security Assessment & Authorization Version 1.1,* Revision Date July 2019
d. SI Technical Note IT-930-TN33, *Vulnerability Management Program,* last revised August 29, 2019

Incident Response

a. SI Technical Note IT-930-TN30, *IT Security Incident Response Plan and Procedures,* June 18, 2018

Contingency Planning

a. NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems,* May 2010
b. SI Information Technology Technical Standards & Guidelines IT-960-02, *IT Disaster Recovery Planning Version 2.0*, June 2019
c. *NMAI Collections Information System Contingency Plan/Disaster Recovery Plan*, July 2019
d. *PANDA Contingency Plan Disaster Recovery Plan,* May 2019
e. *Infrastructure Disaster Recovery Plan "High Level Common Components,"* January 2018

APPENDIX B – FISCAL YEAR 2019 CYBERSCOPE REPORT

Overall	
FISMA Question	**FY2019 Assessment**
0.1 - Please provide an overall IG self-assessment rating (Effective/Not Effective).	Overall Level 2: Defined – Not Effective
0.2 - Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.	Williams Adley selected the Smithsonian Institution general supp two major systems out of 38 major systems and general support s detailed testing for the FY 2019 FISMA audit. Overall, the Smithsonian Institution has made progress in address identified information security deficiencies. It has created an info architecture, updated policies and procedures in all functions, cor of all SI information systems, and completed the implementation Security Continuous Monitoring (ISCM) strategy. The Smithsoni Information Officer has several initiatives to continue improving security posture of the Smithsonian. However, Smithsonian Instit process of authorizing or re-authorizing 23 of 38 major systems. that has recently gone through the new authorization process did configuration management plan. Based on the assessment of Smithsonian Institution's information overall maturity level is Level 2, *Defined*. The Department of Ho Office of Management and Budget, and the Council of the Inspec Integrity and Efficiency considers Level 4, Managed and Measur level at the metric, domain, function and overall security program

Function: Identify – Risk Management	
FISMA Question	**FY2019 Assessment**
1 - To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including	**Level 2: Defined** – Smithsonian Institution has defined proc the Authorization to Operate (ATO) package for all informa However, Smithsonian Institution is in the process of identi

cloud systems, public facing websites, and third-party systems), and system interconnections (NIST SP 800- 53. Rev. 4: CA-3, PM-5, and CM8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2019 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).	comprehensive and accurate inventory of its information systems and system interconnections. Specifically, one (1) of two (2) selected systems did not document all its interconnections in its System Security Plan in FY 2019; the missing interconnection was added to the System Security Plan after the FY 2019.
2 - To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2019 CIO FISMA Metrics: 1.2 and 3.9.2; CSF: ID.AM-1).	**Level 2: Defined** – Smithsonian Institution has defined a process for using standard data elements/taxonomy to develop and maintain a Systems Application Based Inventory, and a defined process for how to add a hardware inventory items into the GRC. However, Smithsonian Institution did not have an up-to-date accurate GSS hardware inventory list documented for Herndon Data Center. Based on Williams Adley's observation of the 25 out of 1,701 sampled hardware inventory tested, we have determined that one (1) server was not accurately documented for its current location. Additionally, Smithsonian Institution did not have a complete hardware inventory listing as 23 of 38 of its information systems were in the process of getting re-authorized. Furthermore, OCIO did not maintain a complete list of hardware component inventories.
3 - To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2019 CIO FISMA Metrics: 3.10.1; CSF: ID.AM-2).	**Level 2: Defined** – Smithsonian Institution has defined a process for using standard data elements/taxonomy to develop and maintain a Systems Application Based Inventory, and a defined process for how to add a software inventory items into the GRC. However, Smithsonian Institution did not have a complete software inventory or software license inventory listing as 23 of 38 of its information systems were in the process of getting re-authorized. Additionally, OCIO did not maintain a complete list of software component inventories.
4 - To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM11; NIST SP 800-	Smithsonian Institution has categorized and communicated the importance/priority of information systems in enabling its missions and business functions. Smithsonian Institution has also defined the importance/priority levels for its information systems and how to consider risks for supporting business functions and mission impact. Additionally, Smithsonian Institution has rated IT security as one of the top 25 risks to the agency.

60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2019 CIO FISMA Metrics: 1.1; OMB M-19-03).	However, Smithsonian Institution is still in the process of re-authorizing all information systems.
established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800- 39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 – 2; SECURE Technology Act: s. 1326)?	**Level 2: Defined** – Smithsonian Institution has defined and communicated its risk management policies, procedures, and strategy. Smithsonian Institution also has established a risk management committee charter that was established in FY 2014, which states that the committee shall meet at least four times a year. However, as Smithsonian Institution is in the process of redefining the charter, only two risk management committee meetings were held in FY 2019 with documented agendas instead of meeting minutes. As Smithsonian Institution is updating the risk management process, more defined meeting frequencies will be established along with the implementation of more robust communication of risks through meetings and workshops in FY 2020.
6 - To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA9, SA-12, and PM-9; NIST SP 800-161; CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326).	**Level 2: Defined –** Smithsonian Institution has defined and implemented the information security continuous monitoring strategy. However, Smithsonian Institution did not establish a defined information technology security architecture until July 2019, therefore it was not in place to provide information security discipline and structure for nine (9) of 12 months in FY 2019.
7 - To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security	Smithsonian Institution has defined roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders. These key individuals have been

Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?	performing the roles and responsibilities that have been defined across the organization. However, Smithsonian Institution has an established risk management committee charter established in FY 2014 that states the committee shall meet at least four times a year; however, only three risk management committee meetings were held in FY 2019 with no meeting minutes documented.
8 - To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?	Smithsonian Institution has defined policies and procedures for POA&M maintenance, tracking, and review to ensure the POA&Ms have complete information needed to be closed. Smithsonian Institution has consistently implemented POA&Ms, in accordance with the Smithsonian Institution's policies and procedures, to effectively mitigate security weaknesses. However, Smithsonian Institution has not implemented a measuring mechanism to measure the effectiveness of an overall POA&M management program.
9 - To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2)).	**Level 2: Defined** – Smithsonian Institution has a defined Information Security Risk Assessment procedure that includes threats, vulnerabilities, and impacts. However, as Smithsonian Institution is still in the process of re-authorizing their information systems, risk assessments have not been completed for 23 of 38 information systems that were still pending re-authorization by the end of FY 2019.
10 - To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-	Smithsonian Institution has defined how information security risks are communicated to all necessary internal and external stakeholders. Additionally, Smithsonian Institution has communicated information about risks in a timely and consistent manner to all internal and

123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326).	external stakeholders with a need-to-know. Currently, Smithsonian Institution is in the process of updating an existing Smithsonian Risk Committee Charter, there will be regular Risk Committee meetings hosted at least four times per year. In FY 2019 the Risk Committee met three times, however, it was determined that they are adjusting the process. There is a monthly IT Security meeting where risks are discussed. In addition, the CIO briefs the audit committee on a regular basis on IT security risks.
11 - To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting *contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800- 152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).*	Smithsonian Institution has defined policies and procedures that require specific security FAR clauses, clauses on protection of PII and reporting of information as well as requirement of erconnection security agreement to be completed. Additionally, Smithsonian Institution has ensured that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. However, Smithsonian Institution has not fully implemented the use of qualitative and quantitative performance metrics to measure, report on, and monitor information security performance of contractor-operated systems and services in FY 2019.
12 - To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook).	Smithsonian Institution has obtained and began implementation of a Governance, Risk and Compliance (GRC) tool, to provide a centralized view of risks across the entity's information systems. However, not all information systems have been completed the ATO process with required details included in the GRC, therefore SI could not fully manage and measure all risks at the end of FY 2019. Additionally, not all systems have gone through the risk assessment process, as 23 of 38 systems have not been re-authorized by the end of FY 2019.
13 - *effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated*	Smithsonian Institution has consistently implemented the GRC, a governance, risk, and compliance tool, and re-authorizing of all information systems. However, as of the end of FY 2019, 23 of 38 systems had not yet been re-authorized using the new process. As such, the risk management process,

from the questions above and based on all testing performed, is the risk management program effective.	including risk identification, control, and monitoring, has not been consistently implemented for all major systems.
Calculated Maturity Level	**Level 2: Defined**
Overall Function Maturity Level	**Level 2: Defined**

Function: Protect – Configuration Management	
FISMA Question	**FY2019 Assessment**
14 - To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800- 128: Section 2.4).	**Level 2: Defined** – Smithsonian Institution has defined roles and responsibilities for configuration management stakeholders. However, OCIO did not update all of its configuration management policy documents within the defined timeframe, specifically, defined roles and responsibilities for configuration management stakeholders were outdated in IT-960-TN01 Change Management during FY 2019. IT-960-TN01 was last updated in 2013 was used throughout FY 2019. OCIO has updated the defined roles and responsibilities for configuration management stakeholders, as noted in the change log in IT-960-TN01 on October 7, 2019. In addition, one of two information systems tested have not developed a configuration management plan, as required.
15 - To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9).	**Level 2: Defined** – Smithsonian Institution has defined entity-level configuration management policies and procedures for the GSS. However, for five (5) of eight (8) sampled changes tested for one (1) of the two (2) selected information systems did not have proper management signoff before development and testing were done for changes, in accordance to the system's Operations Guide. The system's management has updated this process in FY 2020.

16 - To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM1; NIST SP 800-128: 2.2.1).	**Level 2: Defined** – Smithsonian Institution has defined and dispersed comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements. However, one (1) of two (2) in-scope selected systems did not consistently implement the requirement to have defined system level CM procedures.
17 - To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM8; FY 2019 CIO FISMA Metrics: 1.1, 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1).	Smithsonian Institution has defined and dispersed its baseline configuration and component inventory procedures. However, Smithsonian Institution did not have an up-to-date accurate hardware inventory list documented for Herndon Data Center. Based on Williams Adley's observation of the 25 out of 1701 sampled hardware inventory items tested, we have determined that one (1) server was not accurately documented for its current location.
18 - To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, and SI-2; FY 2019 CIO FISMA Metrics: 1.1 and 2.2; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8).	**Level 2: Defined** – Smithsonian Institution has defined baseline configurations at the system-level. However, the Smithsonian Institution does not have a complete list of the hardware and software inventory to ensure baselines are implemented across the entity. Additionally, 23 of 38 systems have not been re-authorized and tracked in the GRC.
19 - To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3 and SI-2; NIST SP 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20, Control 4.5; FY 2019 CIO FISMA Metrics: 2.13; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02).	**Level 2: Defined** – Smithsonian Institution has defined remediation processes, including patch management, to manage software vulnerabilities. However, 234 high to very high vulnerabilities identified in November 2018 continued to be identified in June 2019. Additionally, OCIO implemented a new process to ensure vulnerabilities were addressed in a timely fashion, however, it was not in place for seven (7) of 12 months in FY 2019.

20 - To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-08-05)?	Smithsonian Institution has chosen not to implement TIC as it is not applicable to their environment. However, Smithsonian Institution has taken measures to protect its network by blocking external connections and by implementing the Uniform Resource Locator (URL) filtering policy for external connections.
21 - To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change *configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2 and CM-3; CSF: PR.IP-3).*	**Level 2: Defined** – Smithsonian Institution has defined change control policies and procedures. However, OCIO did not update all its change management policy documents within the defined timeframe, specifically, IT-960-TN01, Change Management, had not been updated for six years. Smithsonian Institution were in the process of updating it in FY 2019, and the update was published subsequent to the end of FY 2019, on October 7, 2019. Additionally, one of two in-scope systems did not have defined policies and procedures regarding the CCB. Furthermore, for five (5) of eight (8) sampled changes tested for one (1) of the two (2) selected information systems did not have proper management signoff before development and testing were done for changes, in accordance to the system's Operations Guide. The system's management has updated this process in FY 2020.
22 - Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective.	Smithsonian Institution has made progress defining and implementing an entity wide configuration management process. However, Williams Adley had identified issues with implementation of configuration management at the individual system level.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Identity & Access Management	
FISMA Question	**FY2019 Assessment**
23 - To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM)).	**Level 3: Consistently Implemented –** Smithsonian Institution has defined roles and responsibilities for identity and access management and has developed an ICAM governance structure to align and consolidate the agency's ICAM investments, monitoring programs, and ensuring awareness and understanding for all stakeholders. Additionally, Smithsonian Institution has ensured that the defined roles and responsibilities have been carried out across the organization.
24 - To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities FICAM.	**Level 2: Defined** – Smithsonian Institution has defined identity and access management strategy. However, the enterprise IT security architecture had not been established until July 2019 to assist the full implementation of the ICAM strategy to guide Smithsonian Institution's ICAM process and activities.
25 - To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5).	**Level 2: Defined** – Smithsonian Institution has defined identity and access management policies and procedures. However, ICAM policies and procedures document, Information Technology Technical Standards & Guidelines IT-930-TN37, Securing IT accounts, has not been updated for four (4) years since its initial release on October 2015 as review is required at least every three years as identified in IT-930-02. Additionally, IT-930-TN37 identifies the need for passwords, length and complexity, but does not detail the required use of two-factor authentication for privileged users.
26 - To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11).	**Level 3: Consistently Implemented** – Smithsonian Institution has defined procedures for screening and assigning personnel risk designation. However, Smithsonian Institution has not implemented an automated tool that shares assigned risk designations across the organization to those who need to know.
27 - To what extent does the organization ensure that access agreements, including nondisclosure	**Level 3: Consistently Implemented –** Smithsonian Institution has defined its processes for developing, documenting, and maintaining access agreements for

agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800- 53 REV. 4: AC-8, PL-4, and PS6)?	individuals that access the Smithsonian network. However, one (1) of 22 sampled GSS users did not have user agreements within the required time frame, however they did have a screenshot that HR collected the form when the user came on. Smithsonian Institution does not have process to centrally collect and maintain user agreement forms.
28 - To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?	Smithsonian Institution has implemented a strong authentication for all remote and email cloud access. However, Smithsonian Institution has chosen not to implement the use of strong authentication mechanisms for non-privileged users to access its facilities, networks, and systems onsite as it is not an executive branch agency and is not required to have strong authentication for all users in the environment.
29 - To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?	Smithsonian Institution has implemented strong authentication, Entrust security token, for all users for remote access and for privileged users who are Tier 0. Smithsonian Institution has not yet implemented, but has planned for the, use of strong authentication mechanisms for other privileged users to access its facilities, systems, and networks.
30 - To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged	**Level 2: Defined** – Smithsonian Institution has defined a process for provisioning, managing and reviewing privileged accounts. However, aside from dormant account checks, two (2) of two (2) selected information systems do not periodically review privileged user account activities.

user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).	
31 - To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10).	**Level 2: Defined** – Smithsonian Institution has defined its configuration requirements for remote access connections. However, there is no defined policies and procedures for the review of audit logs, including a list of defined auditable events, of activities by remote users using VPN or Citrix. Nevertheless Citrix and VPN logs are sent to the SIEM, which has alerts that cover remote access activities.
32 - Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?	Smithsonian Institution has made progress with the implementation of two-factor authentication for enterprise administrators and ensuring the defined roles and responsibilities for identity and access management are carried out throughout the institution. However, access agreements for individuals that access the Smithsonian network were not properly maintained, privileged user account activities were not reviewed on a system level, and not all ICAM policies and procedures were up to date throughout FY 2019.
Calculated Maturity Level	**Level 3: Consistently Implemented**

Function: Protect – Data Protection and Privacy	
FISMA Question	**FY2019 Assessment**
33 - To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used,	**Level 3: Consistently Implemented** – Smithsonian Institution has defined a privacy program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems. Additionally, Smithsonian

maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J).	Institution consistently implements its privacy program by maintaining an inventory of the collection and use of PII, conducting; maintaining privacy impact assessments; and reviewing and removing unnecessary PII collections on a regular basis. However, Smithsonian Institution has not completed all Privacy Assessments (PA) for its information systems.
34 - To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)? *• Encryption of data at rest* *• Encryption of data in transit* *• Limitation of transfer to removable media* *• Sanitization of digital media prior to disposal or reuse*	**Level 2: Defined** – Smithsonian Institution has defined security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle including the use of encryption of data at rest, data at transit and limits to removable media. However, Smithsonian Institution has not consistently implemented the security control for encryption of data in transit to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle. Specifically, while encryption is in place for transmission of sensitive information, many systems in the SI enterprise that were using vulnerable SSL and TLS versions, OCIO is still working on the migration of all systems to TLS 1.2. With this endeavor, SI is migrating from Windows 7 to pleted in the beginning of FY 2020.
35 - To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5).	**Level 2: Defined** – Smithsonian Institution has defined security controls to prevent data exfiltration and enhance network defenses. Smithsonian Institution has also begun to implement and harden the Microsoft Anti-Malware solution in late April of 2019 to prevent data exfiltration, specifically, SI has configured malware notifications for internal sources and schedule malware and spam reports to run automatically. However, data loss prevention function in the Microsoft 365 is only implemented for Human Resource unit to prevent data loss, for all other Smithsonian Institution units, it notifies SI of a possible violation or data exfiltration after the policy has been violated.
36 - To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25).	**Level 2: Defined** – Smithsonian Institution has defined a Data Breach Response Plan which is informed and supported by the Smithsonian Privacy Principles found in SD 118 – Privacy Policy. However, Smithsonian Institution has not conducted tabletop exercises, or any lessons learned to make improvements to the plan as appropriate in FY 2019.

37 - To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role based privacy training (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements).	**Level 3: Consistently Implemented** – Smithsonian Institution has defined privacy awareness training policies and procedures. Smithsonian Institution has also ensured that all individuals receive basic privacy awareness training and individuals having responsibilities for PII or activities involving PII receive role-based privacy awareness training. At the end of FY 2019, Smithsonian Institution is in the process of incorporating more PII training into the annual Computer Security Awareness Training (CSAT) training material so the additional privacy training material will automatically be included as part of the annual CSAT training.
38 - Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective.	Smithsonian Institution has made progress to reduce the number of PII holdings, identify all systems requiring an PA, ensured that privacy awareness training is provided to all individuals and initiated periodic privacy reviews of IT systems in FY 2019. However, Smithsonian Institution has not consistently implemented the security control for encryption of data in transit, conducted tabletop exercises or any lessons learned to make improvements to the plan as appropriate in FY 2019. Additionally, there are areas, identified above, that can be improved, including continue to update SD 118, Privacy Policy, implement more privacy training for all staff across the organization, and ensure that Privacy Assessments are completed for all information systems.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Security Training	
FISMA Question	**FY2019 Assessment**
39 - To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and	**Level 4: Managed and Measurable** – Smithsonian Institution has defined and communicated roles and responsibilities for stakeholders involved in the security awareness and training program. In addition, stakeholders have adequate resources (people, processes, and technology) to consistently implement security awareness and training responsibilities. Additionally, Smithsonian Institution IT training budget is established for enterprise-wide CSAT training as well as their

training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800- 53 REV. 4: AT-1; and NIST SP 800-50).	role-based training, such as PCI certification and additional elevated privileged training.
40 - To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800- 50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?	**Level 2: Defined –** There is no defined policies and formal procedures in place for assessing the knowledge, skills, and abilities of SI's workforce and specifically for gap remediation. However, Smithsonian Institution has performed an informal skill gap assessment in FY 2019 and documented the results.
41 - To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT1).	Smithsonian Institution has focused on tailoring its annual security awareness training and conducts internal review of all trainings annually to determine appropriateness. Smithsonian Institution has also consistently implemented its organization-wide security awareness and training strategy and plan. However, Smithsonian Institution has not implemented the analysis of the effectiveness of its training strategies and plans in FY 2019.
42 - To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of	**Level 4: Managed and Measurable** – Smithsonian Institution has defined and implemented security awareness and specialized security training policies and procedures. Smithsonian also monitors and analyzes qualitative and quantitative

questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).	performance measures on the effectiveness of its security awareness and training policies and procedures. Smithsonian Institution ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. Smithsonian Institution is able to provide evidence of tracking metrics related to security awareness and training activities. However, two (2) of 22 GSS users tested did not complete their CSAT training within the required timeframe, this was due to an error in system configuration – so both users missed the deadline. Smithsonian Institution resolved the configuration error as soon as the error was ed the users completed their CSAT training within 30 days of resolution.
43 - To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).	**Level 4: Managed and Measurable** – Smithsonian Institution tailors security awareness training specifically to match the requirements identified as critical by the OCIO. OCIO measures the effectiveness of its awareness training program by, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate. Phishing exercises work by sending the user phishing emails multiple times.
44 - To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?	**Level 3: Consistently Implemented** – Smithsonian Institution ensures individuals with significant security responsibilities are provided specialized security training prior to information system access or performing assigned duties and periodically thereafter and maintains appropriate records for Privileged User Security Training (S-111). However, one (1) out of one (1) privileged user tested for one (1) of two (2) selected systems did not take S-111 within 30 days of the user obtaining a role as the system's Administrator as required, OCIO did not receive the notification from the unit that this user was a

	privilege user because the unit did not identify this user as an elevated privilege user, so the user was not tracked as an elevated user.
45 - Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?	The Smithsonian Institution has implemented the policies and procedures. The skill gap assessment was not formally conducted in FY 2019. Additionally, Security training is tracked and monitored in real time. Williams Adley determined that Smithsonian Institution's overall security training program is at Level 4, Managed and Measurable.
Calculated Maturity Level	**Level 4: Management and Measurable**
Overall Function Maturity Level	**Level 2: Defined**

Function: Detect – Information Security Continuous Monitoring	
FISMA Question	**FY2019 Assessment**
46 - To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization wide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?	**Level 3: Consistently Implementing** – Smithsonian Institution has defined an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities and is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. However, Smithsonian Institution did not integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization at the system level. Additionally, 23 of 38 information systems have not completed the re-authorization process for Smithsonian Institution to consistently ensure an organization wide approach to ISCM.
47 - To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls;	**Level 3: Consistently Implemented** – Smithsonian Institution has defined information security continuous monitoring policies and procedures to support the ISCM strategy and has conducted POA&Ms for selected systems at the program level and has consistently implemented the lessons learned process.

collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?	However, Smithsonian Institution has 23 of 38 information systems which have not completed the re-authorization process.
48 - To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics).	**Level 3: Consistently implemented –** Smithsonian Institution has defined ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies. Smithsonian Institution has allocated budget to IT security.
49 - How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03).	**Level 2: Defined** – Smithsonian Institution has defined a process for performing ongoing assessments, granting system authorizations, and monitoring security controls. However, ongoing assessments were not implemented for 23 of 38 information systems, which are in the process of being re-authorized. Additionally, the SSP for one (1) of two (2) selected systems did not have all interconnection systems documented.
50 - How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?	**Level 2: Defined** – Smithsonian Institution has defined an ISCM strategy which identified a list of various security and operational dashboards being used to monitor metrics on an entity level. However, there is no defined process to monitor and analyze all the metrics, and not all identified metrics have been setup in FY 2019.
51 - Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?	Smithsonian Institution has made progress to continuously monitor information security in FY 2019. However, some of the areas above ISCM program could be improve on at the system level, including the SIEM needs to be fully implemented to provide system-specific dashboards across the enterprise for monitoring correlated threat data on a system level.

Calculated Maturity Level	**Level 3: Consistently Implemented**
Overall Function Maturity Level	**Level 3: Consistently Implemented**

Function: Respond – Incident Response	
FISMA Question	**FY2019 Assessment**
52 - To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).	**Level 2: Defined** – Smithsonian Institution has defined and communicated incident response policies, procedures, plans, and strategies. However, two of two information systems selected did not consistently implement up-to-date incident response policies and procedures throughout FY 2019 before implementing the current one on May 17, 2019 for one (1) of two (2) selected information systems and July 2019 for the other one (1) of two (2) selected systems.
53 - To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?	**Level 2: Defined** – Smithsonian Institution has defined and communicated the structures of its incident response teams, roles, and responsibilities of incident response stakeholders, and associated levels of authority and dependencies. However, one (1) of two (2) in-scope systems, has not defined and communicated the structures of its incident response teams, roles, and responsibilities of incident response stakeholders, and associated levels of authority and dependencies.
54 - How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS8; and US-CERT Incident Response Guidelines).	**Level 2: Defined** – Smithsonian Institution has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. Policies and procedures are in place for supporting technologies used to detect/analyze potential incidents. However, three (3) of four (4) sampled security incidents were not categorized with impact levels in a timely manner, therefore, the proper impact level assignment was delayed.
55 - How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2).	**Level 2: Defined** – Smithsonian Institution has defined processes for incident response plan to include: containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and

	mitigate any vulnerabilities that were exploited, and recovery of systems. However, after Smithsonian attempted to mitigate a fraudulent transaction incident that occurred in FY 2018, the security issue still persisted and continued to impact some Smithsonian websites in April 2019. In addition, three (3) of four (4) sampled security incidents were not categorized with impact levels in a timely manner, therefore, the proper impact level assignment was delayed.
56 - To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message).	**Level 2: Defined** – Smithsonian Institution has defined its requirements for personnel to report suspected security incidents to the entity's help desk and/or security operations center within the defined timeframes. In addition, Smithsonian Institution has defined its processes for reporting security incidents to US-CERT. However, in FY 2019, three (3) of four (4) sampled security incidents were not categorize with impact levels in a timely manner, therefore, the proper impact level assignment was delayed.
57 - To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR4; OMB M-18-02; PPD-41).	Smithsonian Institution is not required to have a contract with DHS for Einstein implementation. Smithsonian Institution has a contract with Fortinet to implement the technical assistance capabilities similar to what Einstein can provide, which can be leveraged for quickly responding to incidents, and more suitable for Smithsonian Institution.
58 - To what degree does the organization utilize the following technology to support its incident response program? • *Web application protections, such as web application firewalls* • *Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools*	**Level 2: Defined** – Smithsonian Institution has utilized incident response tools including email anti-malware and host based anti-malware to support the incident response program. However, while tools are implemented to support some incident response activities, Smithsonian Institution did not consistently utilize its technologies as incident response process for FY 2019. Specifically, the data loss prevention function in the Microsoft 365 only works for the Human Resource unit to prevent data loss, for all other Smithsonian Institution units, it notifies SI of a possible violation after the policy has been violated.

• *Aggregation and analysis, such as security information and event management (SIEM) products* • *Malware detection, such as antivirus and antispam software technologies* • *Information management, such as data loss prevention* *File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44).*	
59 - Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?	Smithsonian Institution has implemented an email anti-malware and host based anti-malware tools to support incident response activities. In addition, Smithsonian Institution made progress to automatically report security incidents to internal and external stakeholders There are areas, identified above, that can be improved, such as reporting incidents to the external stakeholder in a timely manner.
Calculated Maturity Level	**Level 2: Defined**
Overall Function Maturity Level	**Level 2: Defined**

Function: Recover – Contingency Planning	
FISMA Question	**FY2019 Assessment**
60 - To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B).	**Level 3: Consistently Implemented -** Smithsonian Institution has a defined IT Disaster Recovery Planning document where defined roles and responsibilities. By inspecting FY 2019 Disaster Recovery Test Report, we noted that individuals performing the roles and responsibilities participated during the exercise. Therefore, the roles and responsibilities were consistently implemented.
61 - To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and	**Level 2: Defined** – Smithsonian Institution has defined ISCP policies and procedures. However, Smithsonian Institution could not consistently implement its information system contingency planning program as two (2) of two (2)

strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).	selected information systems did not have a system-specific business impact analysis (BIA) documented in the system-specific DRP. Additionally, two of the two in-scope information systems selected did not have recovery time objectives or recovery point objectives defined.
62 - To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4).	**Level 2: Defined –** Smithsonian Institution has defined a process for conducting a system level business impact analyses in according to IT-960-02, IT Disaster Recovery Planning, and has begun to conduct business impact analyses using the GRC to guide contingency planning efforts at the entity level. However, two (2) of the two (2) information systems selected do not have system-specific BIAs documented in the systems' recovery plan.
63 - To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9).	**Level 2: Defined** – Smithsonian Institution has defined a process for conducting a business impact analyses in according to IT-960-02, IT Disaster Recovery Planning, and has begun to conduct business impact analyses using the GRC to guide contingency planning efforts at the entity level. However, as two (2) of the two (2) information systems selected do not have system-specific BIAs documented in the systems' recovery plan, recovery point or recovery time objectives as required.
64 - To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10).	**Level 2: Defined** – Smithsonian Institution has a defined process to perform tests/exercises of its information system contingency planning. However, for one (1) of two (2) selected information systems, no contingency plan testing was conducted in FY 2019, as required.
65 - To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?	**Level 3: Consistently implemented** – Smithsonian Institution has consistently implemented its processes, and technologies for information system backup and storage, including the use of alternate storage and processing sites and RAID, as appropriate. Alternate processing and storage sites are chosen based upon risk assessments which ensure the potential disruption of the Smithsonian Institution's ability to initiate and sustain operations is minimized and are not subject to the same physical and/or cybersecurity risks as the primary sites. Additionally, backups of information at the user-and system-levels are

	consistently performed and the confidentiality, integrity, and availability of this information is maintained.
66 - To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk-based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR4)?	**Level 2: Defined** – Smithsonian Institution has defined an infrastructure information system contingency plan that addresses roles and responsibilities as well as communication requirements and an up-to-date phone tree. Additionally, there is a developed disaster recovery plan for critical systems housed in the data center with roles and responsibilities and communication processes. However, one (1) of two (2) selected in-scope information systems, did not conduct annual contingency plan testing in FY 2019, as required.
67 - effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?	Smithsonian Institution made progress updating and implementing an entity wide IT Disaster Recovery Planning document and has conducted an entity level BIA in FY 2019. There are areas, identified in the previous metric questions, that can be improved upon, including ensuring that each system has its recovery time objective and recovery point objective included in the system-specific DRP and conducting annual contingency plan testing.
Calculated Maturity Level	**Level 2: Defined**
Overall Function Maturity Level	**Level 2: Defined**

APPENDIX C – SYSTEM DESCRIPTIONS

Williams Adley presents the following information on each of the three systems that were evaluated as part of the FY2019 Information Security Program Review:

1. SINet, SI's General Support System (GSS), includes network transport, network security, and shared infrastructure that provides core capability to SI's other major applications and miscellaneous information technology (IT) systems that support SI's mission and objectives. The shared infrastructure consists of the hosting environment (servers), multiple productivity applications (e.g., Email, SharePoint, Communication Services), SI websites, remote access (i.e., VPN and Citrix), and the end users' desktop environment. The system and its data are assessed and categorized as Moderate.

2. Pan-Institutional Database for Advancement (PANDA), one of SI's Moderate applications, is the database of record for Smithsonian donations. It contains the gift, pledge, matching gift, and membership transactions for the central Office of Advancement (OA) and the units. The system contains PII data that includes donors' contact information, such as address, email, and telephone number.

3. National Museum of the American Indian Collections Information System (NMAI-CIS), one of SI's Moderate applications, is used to manage the assets that the museum holds in trust for the Nation. NMAI-CIS currently provides a central repository for the Objects and Photographic Archives collections and for about 5.6 terabytes (TB) of images for these collections.

APPENDIX D – INSPECTOR GENERAL FISMA METRICS

In response to the increasing concern related to cybersecurity, President Obama issued Executive Order (EO) 13636, which requires development of a set of industry standards and best practices to help organizations manage information security risks to meet cybersecurity challenges. One (1) result of EO 13636 was development of the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity."[10] This framework provides guidelines for organizations to protect their critical infrastructure by using business drivers to direct information security activities and to consider information security risks as part of the organization's risk management processes.

To emphasize the importance of protecting critical infrastructure, President Trump issued EO 13800, which holds agency heads responsible for managing cybersecurity risk in their organizations. Specifically, EO 13800 defines effective risk management as requiring agency heads to lead integrated teams of senior executives who have expertise in IT, security, budgeting, acquisition, law, privacy, and human resources. EO 13800 also requires agency heads to use the framework to manage the agencies' cybersecurity risk and holds agency heads accountable for ensuring that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

Accordingly, on April 9, 2019, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) released the "FY2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.3." FISMA requires each agency IG to annually conduct an independent evaluation of the information security program and practices of its respective agency. This guidance comprises eight (8) IG FISMA metrics domains that are organized around the five (5) information security functions outlined in the framework, as follows:

1. *Identify Function*

   Risk Management Domain—The purpose of the risk management domain is to evaluate the maturity of an agency's risk management program. An agency with an effective risk management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.

2. *Protect Function*

   Configuration Management Domain—The purpose of the configuration management domain is to evaluate the maturity of an agency's configuration management program. An agency with an effective configuration management program uses automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes,

[10] NIST, *Framework for Improving Critical Infrastructure Cybersecurity version 1.1,* April 2018.

and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.

Identity and Access Management Domain—The purpose of the identity and access management domain is to evaluate the maturity of an agency's identity and access management program. An agency with an effective identity and access management program ensures that all privileged and non-privileged users use strong authentication to access organizational systems; uses automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its identity, credential, and access management program.

Data Protection and Privacy Domain—The purpose of the data protection and privacy domain is to evaluate the maturity of an agency's data protection and privacy program. An effective data protection and privacy program enables an agency to ensure protection of its PII and other agency-sensitive data throughout the data lifecycle; respond to privacy events; develop and maintain enhanced network defenses; and monitor, analyze, and report qualitative and quantitative performance measures on the effectiveness of its data protection and privacy program.

Security Training Domain—The purpose of the security training domain is to evaluate the maturity of an agency's security training program. An agency with an effective security training program addresses all of its identified knowledge, skills, and abilities gaps; measures the effectiveness of its security training program; and ensures staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of its security awareness and training activities.

3. *Detect Function*

Information Security Continuous Monitoring (ISCM) Domain—The purpose of the ISCM domain is to evaluate the maturity of an agency's ISCM program. An agency with an effective ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

4. *Respond Function*

Incident Response Domain—The purpose of the incident response domain is to evaluate the maturity of an agency's incident response program. An agency with an effective incident response program uses profiling techniques to measure the characteristics of expected activities on its network and systems so that it can more effectively detect security events; manages and measures the impact of successful events; uses incident response metrics to manage and measure the timely reporting of incident information to organizational officials and external stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.

5. *Recover Function*

Contingency Planning Domain—The purpose of the contingency planning domain is to evaluate the maturity of an agency's contingency planning program. An agency with an effective contingency planning program uses automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of information system contingency planning program activities.

APPENDIX E – ACRONYMS

AIS	Advancement Information System
BIA	Business Impact Analysis
CCB	Change Control Board
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIS	Collections Information System
CM	Configuration Management
CSAT	Computer Security Awareness Training
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	United States Department of Homeland Security
DLP	Data Loss Prevention
DPP	Data Protection and Privacy
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning
FAR	Federal Acquisition Regulation
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk, and Compliance
HR	Human Resources
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IP	Internet Protocol
ISCM	Information Security Continuous Monitoring
ISSO	Information Systems Security Officer
IT	Information Technology
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
NMAI	National Museum of the American Indian
OA	Office of Advancement
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PANDA	Pan-Institutional Database for Advancement
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Directive

RPO	Recovery Point Objective
RTO	Recovery Time Objective
SD	Smithsonian Directive
SE	Smithsonian Enterprise
SI	Smithsonian Institution
SIEM	Security Information and Event Management
SINet	Smithsonian Institution Network
SLA	Service Level Agreement
SOC	Security Operations Center
SP	Special Publication
sPII	Sensitive Personally Identifiable Information
SPO	Smithsonian Privacy Office
SSL	Secure Sockets Layer
SSP	System Security Plan
TIC	Trusted Internet Connection
TLS	Transport Layer Security
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

APPENDIX F – MANAGEMENT'S COMMENTS

Smithsonian Institution

Office of the Chief Information Officer

Date: September 18, 2020

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer *Deron Burba* 9/18/2020 | 3:53 PM EDT

CC: Mike McCarthy, Undersecretary for Finance and Administration
Doug Hall, Acting Deputy Under Secretary for Finance & Administration
Greg Bettwy, Chief of Staff
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Joan Mockeridge, Office of Inspector General
Celita McGinnis, Office of Inspector General
Juliette Sheppard, Director of IT Security
Danee Gaines Adams, Privacy Officer
Carmen Iannacone, Chief Technology Officer
Melanie Dann, Director, Advancement Operations and Systems
Kara Lewis, NMAI CIS System Owner
Erin Bordeaux, NMAI Assistant Director for Information Technology
Stone Kelly, Office of Planning, Management and Budget

Subject: Management Response to "*Report on the Smithsonian Institution's Information Security Program Fiscal Year 2019*"

Thank you for the opportunity to comment on the report. Management agrees with most of the recommendations and has already taken action to implement them.

Recommendation 1: Perform timely reviews and update policies and procedures at the required frequency, in accordance with IT-930-02, Security Controls Manual, Version 4.2f or IT-930-TN37, Securing IT Accounts and SD118, Privacy Policy.

Management concurs with this finding. In FY20, the Office of the Chief Information Officer (OCIO) reviewed all of its important policy and procedure documents and updated the ones that needed changes or were due for revision. More than 40 OCIO policy/procedure/strategy documents related to computer security and privacy were updated this year, including IT-930-TN37 and SD 118. Additionally, required procedure documents were reviewed and developed or updated for each of the major systems. Management considers this recommendation completed.

Recommendation 2: Remediate high vulnerabilities in a timely manner.

Management concurs with this finding. The Smithsonian Institution (SI) has dramatically reduced

both the number of vulnerabilities within the SI environment and the average time to remediate vulnerabilities. SI implemented the un-remediated vulnerability escalation process in August 2019 to help ensure vulnerabilities are addressed in a timely manner. In FY20, SI prioritized remediating high vulnerabilities on servers and several rounds of vulnerability escalations. This has resulted in no remaining high exploitable server vulnerabilities greater than 30 days. OCIO also aggressively targeted workstation vulnerabilities through enhanced configuration management procedures, communications and reporting, new software deployment tools, training, and focusing additional personnel resources. These activities have greatly reduced risk. However, additional time is needed to fully bring remaining asset types in compliance with the remediation timeframe goals. Management expects the remaining work to be completed by August 31, 2021.

Recommendation 3: Develop a process to review change tickets to verify that all system changes are documented, approved, and tested before migrating the changes to production.

Management does not concur with the details of the finding but has made improvements related to the recommendation. OCIO provided information to the auditors to show that the observations called out some tickets that were either not change tickets or change tickets that were cancelled. The other change tickets did have testing results that met the requirements of the Change Control Board (CCB). Although OCIO did not concur with the finding, we continued to make improvements in FY20 which align with the recommendation. This included migrating the CCB process to ServiceNow (SN). The SN workflow enforces change management requirements in compliance with ITIL best practices. The CCB (which SN calls the Change Advisory Board) tracks all new Change Requests and examines information to notify managers of changes that require their approval prior to the requests being presented to the CCB for review and approval. Test results are also enforced by the workflow. Incomplete requests are forwarded back to the owners with requests to provide more detailed information. Lessons learned have led to a ServiceNow KnowledgeBase (KB) Article. The CCB also tracks past due changes and requests that tickets either be updated or closed. Updates are discussed during the CCB meeting to make sure that extensions or changes don't have an undue impact to customers. Management considers this recommendation completed.

Recommendation 4: Develop a process to verify that all incidents are properly categorized to ensure all security incidents are reported in a timely manner.

Management concurs with this finding. IT-930-04, *Information Technology Security Incident Management*, has been developed to consolidate and enhance the Smithsonian's computer security incident response (IR) policies and procedures. OCIO also implemented additional automation including a data feed of Splunk and Office365 alerts into the incident management system. The Security Operations Center (SOC) also hired a new dedicated IR analyst. Additional oversight of the IR process has also been implemented. The SOC Lead and IR analyst meet every week to review alerts and incidents to ensure they are being handled correctly and in a timely manner. Management considers this recommendation completed.

Recommendation 5: Develop and conduct privacy-specific tabletop exercises and capture lessons learned.

Management concurs with this finding. The Privacy Office conducted a Privacy Tabletop exercise with members of the Privacy Council (i.e., Under Secretary for Finance and Administration, Assistant Secretary for Communications and External Affairs, General Counsel, Director of Protection Services, Director of Human Resources, Risk Manager, Chief Information Officer, Director of Government Relations, and Smithsonian Enterprises Chief Information Officer) on June 23, 2020. The Privacy Officer documented the Lessons Learned from this exercise and will use it to inform future process improvements. Management considers this recommendation completed.

Recommendation 6: Upgrade all Smithsonian systems currently using Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TLS1.2.

Management concurs with this finding. SI has made significant progress in prioritizing the enforcement of TLS 1.2 within the SI environment. All Windows and Linux systems are either upgraded to TLS 1.2 or have approved risk acceptance waivers to keep versions of TLS lower than 1.2. However, there are a small number of other devices on the network that are still being remediated. Management expects these remaining devices to be addressed by April 30, 2021.

Recommendation 7: Develop a procedure to identify and document system interconnections in the PANDA System Security Plan.

Management concurs with this finding. There is an existing procedure in IT-930-03, *System Security Assessment and Authorization*, for identifying and documenting system interconnections. The one that the auditors identified as missing was due to a misunderstanding. As mentioned on page 12 of the report, the interconnection has now been documented. OCIO has provided additional training to system stakeholders to understand the requirement and implemented further oversight to ensure that interconnections are documented appropriately as part of the QA process. Management considers this completed.

Recommendation 8: Implement a review process to ensure that all system-specific change specifications are approved before they are migrated to the production environment.

Management does not concur with this finding but has made improvements related to the recommendation. The PANDA team approves and maintains documentation of all changes before they are implemented into production and has provided evidence of those approvals. Additionally, preliminary specifications are also approved prior to development work. However, to enhance the process, signoff forms have now been updated to include a specification authorization signoff in addition to the existing final approval signoff. This ensures that the specification signoffs are retained along with the final signoffs. The Operations Guide (Software and Data Management, Application Changes section) has been updated to reflect this change. Management considers this completed.

Recommendation 9: Define roles and responsibilities for key stakeholders in the PANDA system's configuration management policies and procedure.

Management concurs with this finding. The PANDA Operations Guide has been updated to include documentation of Roles and Responsibilities. Management considers this completed.

Recommendation 10: Develop a process to ensure user account activities, and associated audit logs, are reviewed and documented by the PANDA system owner as required by OCIO Technical Note IT-930-TN37, Securing IT Accounts.

Management concurs with this finding. The PANDA team has implemented monitoring and auditing of privileged DB-user accounts and sensitive application activities and has documented this in the Operations Guide, Log Review Section. Management considers this completed.

Recommendation 11: Document and maintain detailed software and hardware inventory lists for the PANDA system consistent with SI policies and procedures.

Management does not concur with this finding. The PANDA team was compliant with SI procedures for the inventory information that they were responsible for maintaining within Archer for their system. As specified in our procedures, the additional information is maintained centrally in other tools managed by OCIO.

Recommendation 12: Conduct and document a system-level BIA that identifies the maximum tolerable downtime (MTD), recovery time objectives (RTO), and recovery point objectives (RPO), and document the MTD, RPO, and RTO in the contingency plans.

Management concurs with this finding. The PANDA Disaster Recovery Plan has been updated to include these items. Management considers this completed.

Recommendation 13: Test and update the NMAI-CIS system contingency plan annually.

Management concurs with this finding. The NMAI-CIS System Disaster Recovery plan was not tested within FY19 due to some scheduling delays but was promptly tested and updated in early FY20. Management considers this completed.

Recommendation 14: Develop and implement NMAI-CIS system-level configuration management policies and procedures.

Management concurs with this finding. NMAI had been following unwritten procedures for configuration management but has now formally documented them. Management considers this completed.

Recommendation 15: Develop a process to ensure user account activities, and associated audit logs, are reviewed and documented by the NMAI-CIS system owner as required by OCIO Technical Note IT-930-TN37, Securing IT Accounts.

Management concurs with this finding. NMAI has developed a privileged user monitoring plan which includes example scripts that are being used to monitor user activities. Management considers this completed.

Recommendation 16: Document and maintain a detailed software and hardware inventory list for the NMAI-CIS system that is consistent with SI policies and procedures.

Management does not concur with this finding. NMAI personnel were compliant with SI procedures for the inventory information that they were responsible for maintaining within Archer for their system. As specified in our procedures, the additional information is maintained centrally in other tools managed by OCIO.

Recommendation 17: Conduct and document a system-level BIA that identifies the maximum tolerable downtime (MTD), recovery time objectives (RTO), and recovery point objectives (RPO), and document the MTD, RPO, and RTO in the contingency plans.

Management concurs with this finding. NMAI updated its Disaster Recovery Plan in October 2019 (early FY20), including incorporating this BIA information. Management considers this completed.

For the recommendations that Management considers completed, evidence of completion has been placed into the OIG Evidence share.