In Brief

Fiscal Year 2020 Independent Evaluation of the Smithsonian Institution's Information Security Program

OIG-A-21-05, July 6, 2021

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 2020.

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 (FISMA).

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 2020, Williams, Adley & Company - DC, LLP (Williams Adley) found that the Smithsonian Institution (Smithsonian) made improvements to its information security program to address previously identified issues and recommendations. However, Williams Adley found that the Smithsonian's information security program still was not effective.

Improvements included finalizing the re-authorization of 34 information systems, and defining the information security architecture. In addition, Smithsonian's Office of the Chief Information Officer (OCIO) started several initiatives to improve its information security posture, including using automated tools to monitor the effectiveness of Smithsonian's security program with the FISMA reporting metrics. For example, the Smithsonian made significant improvements to its Data Protection and Privacy program by creating and reviewing quantitative and qualitative performance measures on the effectiveness of its privacy activities.

However, Williams Adley also identified gaps within governing documents that support the risk management, configuration management, identity and access management, and data protection and privacy programs. For example, Williams Adley noted that the Smithsonian did conduct its first exercise to test the privacy program, but there is no requirement to conduct this on at least an annual basis.

Williams Adley also found that OCIO has not yet finalized all of its performance measurements and supporting processes for configuration management, information security continuous monitoring, incident response, and contingency planning programs.

Overall, Williams Adley found that the improvements made in fiscal year 2020 resulted in four of the five cybersecurity functions improving in their maturity but still not reaching Level 4. One function, Protect, did achieve Level 4 (managed through quantitative or qualitative measurement) for the first time. However, for an information security program to be considered effective overall, at least three of the five functions must achieve Level 4.

What Was Recommended

Williams Adley made five recommendations to enhance information security at the Smithsonian. Management concurred with all five 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

Memo

Smithsonian

Information requiring protection from public dissemination has been redacted from this report in accordance with Smithsonian Directive 807, *Requests for Smithsonian Institution Information*, Exemption 2 and 5 U.S.C. § 552(b)(7)(E).

Date: July 6, 2021

To: Lonnie Bunch, Secretary

Cc: Meroë Park, Deputy Secretary
Doug Hall, Acting Under Secretary for Administration
Allison Wilcox, Acting Deputy Under Secretary for Administration
Deron Burba, Chief Information Officer
Juliette Sheppard, Director, Information Technology Security, OCIO
Carmen Iannacone, Chief Technology Officer, Office of the Chief Information Officer (OCIO)
Danee Gains Adams, Privacy Officer, OCIO
Nancy Bechtol, Director, Smithsonian Facilities
David McCauley, Supervisory Engineering Technician, Smithsonian Facilities
Carol Le Blanc, President, Smithsonian Enterprises (SE)
Grace Clark, Chief Information Officer, SE
Sandi Cheski, Director Project Management and System Operation, SE
Janice Lambert, Chief Financial Officer
Greg Bettwy, Chief of Staff, Office of the Secretary
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Stone Kelly, Program and Budget Analyst, Office of Planning, Management and Budget

From: Cathy L. Helm, Inspector General Cathy L Helm

Subject: *Fiscal Year 2020 Independent Evaluation of the Smithsonian Institution's Information Security Program* (OIG-A-21-05)

This memorandum transmits the final report of Williams, Adley & Company – DC, LLP (Williams Adley) on the fiscal year 2020 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 2020, 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. Williams Adley made five recommendations for Smithsonian management to enhance information security at Smithsonian. Management concurred with all five recommendations.

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 2020

CONTENTS

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 outlining the result of the performance audit 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, 2020.

FISMA requires each executive branch 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-20-04 ("Memorandum for the Heads of Executive Departments and Agencies: Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements") provides instructions for meeting FY 2020 reporting requirements. We understand that SI is not required to comply with FISMA because it is not an executive branch agency; however, SI applies FISMA standards to its information security program as a best practice to the extent practicable and consistent with its mission.

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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Based on our audit procedures, SI has not met the requirements outlined within the FY 2020 FISMA reporting metrics to be operating at an effective level of security. Furthermore, we determined that SI made improvements to align its governing documents to its existing practices and is working towards developing metrics to evaluate the performance and effectiveness of its information security program and practices.

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 2020 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

June 30, 2021

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 audit firm 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 best practices outlined within the Federal Information Security Modernization Act of 2014 (FISMA). SI is not required to comply with FISMA because it is not an executive branch agency; however, SI applies FISMA standards to its information security program as a best practice to the extent practicable and consistent with its mission.

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 audit of the entity's information security program and to report the results to the Department of Homeland Security (DHS).

OBJECTIVES, SCOPE, AND METHODOLOGY

The SI OIG contracted Williams Adley to evaluate the effectiveness[1] of SI's information security program and practices during the period October 1, 2019 through September 30, 2020 (FY 2020) for a representative sample of SI's information systems[2]. Williams Adley performed this performance audit from June 2020 through October 2020, in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The systems selected for testing are rotated annually among the 34 identified major IT systems and general support systems (GSS). For the FY 2020 audit, the following three (3) SI systems were selected for evaluation:

- **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.
- **Building Automation System (BAS) -** BAS manages secured support for the heating, ventilation, and air conditioning (HVAC) management of air circulation, temperature, and humidity controls to protect collections as well as the comfort of visitors and employees.

[1] Within the context of this report, Williams Adley will make the determination regarding the effectiveness of SI's information security program and practice by utilizing the description outlined within the FY 2020 FISMA reporting metrics and maturity model; "a Level 4, Managed and Measurable, information security program is operating at an effective level of security."

[2] Internal Control deficiencies deemed significant to the objective of the audit (effectiveness of SI's information security program and practices) are discussed within this report.

- **Lawson** - Lawson is an accounting software which consists of the following modules: Accounts Payable, General Ledger, Asset Management, and Activity Management. Lawson is used to generate financial statements, pay non-merchandise vendors, and track expenses.

The three (3) selected systems are categorized by SI as "Moderate[3]" using the Standards for Security Categorization of Federal Information and Information Systems (Federal Information Processing Standards [FIPS] Publication 199[4]). 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 FIPS 199.

To evaluate SI's implementation of its information security program across the selected systems, Williams Adley utilized the FISMA reporting metrics which consists of five cybersecurity framework security functions: Identify, Protect, Detect, Respond, and Recover. These five functions are comprised of 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. A list and description of the five functional areas and eight domains is presented in Appendix D.

The effectiveness of each reporting metric is evaluated on a maturity model spectrum from Level 1: Ad-hoc to Level 5: Optimized. See Table 1 (below) for a description of each level and see Appendix B for the detailed questions. Furthermore, ratings throughout the eight domains will be determined by a simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating.

[3] 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.

[4] SI uses FIPS 199 to determine a system's security categorization.

Table 1: Fiscal Year 2020 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[5] 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: FY 2020 IG FISMA Metrics

In performing this audit, Williams Adley utilized a variety of auditing techniques, including but not limited to:

- Interviewing SI management and employees;
- Inspecting SI policies and procedures and other requested documentation to supplement interviews;
- Conducting judgmental sampling (where applicable); and
- Obtaining sufficient evidence to support our conclusions and recommendations[6].

[5] 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.

[6] For instances where a previously issued recommendation was not addressed and/or a reoccurring issue is identified, Williams Adley will not issue a new recommendation.

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.

THE OFFICE OF THE CHIEF INFORMATION OFFICER

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

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 information security program across SI's information systems. The IT security group is managed by the Director of IT Security, who reports directly to the Chief Information Officer (CIO).

SMITHSONIAN PRIVACY OFFICE

The Smithsonian Privacy Office 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 Smithsonian Privacy Office also works with the units, including the Office of Contracting and Personal Property Management, the Office of Sponsored Projects, and the Office of General Counsel, 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. The 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 DHS, provides guidance on reporting categories and responds to questions for meeting the current fiscal year's reporting requirements.[7] OMB uses the data to carry out its oversight responsibilities and to prepare its annual report to Congress on the entities' compliance with FISMA.

RESULTS OF AUDIT

OVERVIEW

Williams Adley determined that SI has not met the requirements outlined within the FY 2020 FISMA reporting metrics to achieve a Level 4 rating on the maturity model, which is required for an information security program to be determined as operating at an effective level of security.[8] However, it was determined that OCIO consistently implemented processes (Level 3 rating) across all eight (8) FISMA domains. Furthermore, OCIO made improvements to its information security program to address previously identified issues and recommendations, finalized the re-authorization of its information systems, and defined its information security architecture. These improvements resulted in four (4) of five (5) FISMA functions improving in their maturity and one function, Protect, achieving Level 4 for the first time.

In addition, OCIO started several initiatives to continue improving its information security posture, including utilizing data that is monitored and collected by various automated tools to determine the effectiveness of a limited number of controls within its information security program. However, OCIO has not yet finalized all its performance measurements and supporting process to evaluate the overall effectiveness of its information security program.

Based on the result of this FISMA audit, Williams Adley issued five (5) recommendations to assist SI in updating its own policies and procedures to align, where applicable, with best practices outlined in NIST and OMB guidance. Four (4) recommendations are to address the gaps identified within governing documents supporting the risk management, configuration management, and identity and access management programs. In addition, one (1) recommendation is to address the missing performance metrics within the configuration management, incident response, ISCM, and contingency planning programs and assist OCIO with meeting the requirements of an effective information security program under the FISMA maturity model.

---

[7] OMB, *Fiscal Year 2019–2020 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-20-04, November 19, 2019.

[8] 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.

The following sections outline the results of the audit across the five (5) FISMA function areas and eight (8) associated domains.

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.[9] The Identify function is comprised of one (1) domain, risk management, which includes guidance on 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.

Williams Adley determined that in FY 2020, the Identify function operated at Level 3 (Consistently Implemented), an increase of one maturity level since FY 2019.

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

Williams Adley determined that in FY 2020, the risk management program operated at a Level 3 maturity (Consistently Implemented). Specifically, 11 of 12 metric questions were rated a Level 3 maturity and one (1) question rated at a Level 2 maturity.

Overall, the OCIO improved its risk management program by finalizing the re-authorization of its 34 major systems, defining its information security architecture, and modifying its policies and procedures to address historical gaps with existing practices. In addition, the OCIO consistently utilized its plans of action & milestones (POA&Ms) process to mitigate security weaknesses and its automated governance, risk, and compliance (GRC) tool to provide a centralized view of risk.

Although the OCIO made improvements to its risk management program, Williams Adley identified the following two (2) issues; one at the entity level and one at the system level:

Entity-level

(1) OCIO did not maintain complete documentation to demonstrate the execution of its annual IT systems inventory review.

According to SI's IT Security Procedure *Annual* [redacted] *IT Systems Inventory* document, the SI Systems Risk Management (SRM) Team Lead annually sends out a spreadsheet that assists IT System owners and SI Mission Sponsors to validate the SI [redacted] Inventory information for accuracy and completeness. IT System owners and/or SI Mission Sponsors are required to verify

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

the information within [redacted] and provide an updated spreadsheet to the SRM Team Lead outlining the changes made.

As a part of the FY 2020 audit, Williams Adley obtained email correspondences between the SRM Team Lead and the IT System owners and/or SI Mission Sponsors demonstrating communication during the performance of the annual IT systems inventory review. However, documentation was not retained to demonstrate (1) the initial communication from the SRM Team Lead to the IT System owners and SI Mission Sponsors and (2) the updates from the various IT System owners and SI Mission Sponsors.

The OCIO maintained limited documentation to demonstrate the process followed, the results obtained, and the actions taken to address identified issues due to unclear documentation retention requirements within its *Annual* [redacted] *IT Systems Inventory* document.

Without proper documentation, OCIO may not be able to validate whether all gaps within its IT system inventory were resolved and if all IT System owners and SI Mission Sponsors verified their system information within [redacted]

System-level

(2) IT-930-03, *Security Assessment and Authorization Version 1.2*, does not properly indicate where complete hardware and software records for each information system are located.

OCIO's Information Technology Technical Standard & Guideline IT-930-03, *Security Assessment and Authorization Version 1.2*, requires that each major system must have a documented SSP that documents key information such as system description, authorization boundary, component inventory, system interconnections, technical architecture, system categorization, and role designations.

Williams Adley identified inconsistencies between the written Technical Standard & Guideline IT-930-03 and existing practices. OCIO stated that documented SSPs are not used to document hardware and software records as outlined within the Information Technology Technical Standard & Guideline IT-930-03, instead this information is maintained in real time within [redacted]

Without accurate governing documents to guide risk management activities, OCIO risks that the inconsistencies between policy and practice may lead to confusion as to how to obtain accurate information and/or execute security controls.

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.

Williams Adley determined that in FY 2020, the Protect function operated at maturity Level 4: Managed and Measurable, which reflects the Protect function's four (4) domains. During FY 2020, two (2) domains—configuration management and identity and access management operated at

Level 3: Consistently Implemented. The data protection and privacy and security training domain operated at Level 4: Managed and Measurable. Overall, the Protect function increased two (2) maturity levels since FY 2019.

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.

Williams Adley determined that in FY 2020, the configuration management domain operated at Level 3 (Consistently Implemented). Specifically, one (1) metric question was rated a Level 4 maturity, four (4) metric questions were rated a Level 3 maturity, and three (3) metric questions were rated a Level 2.

Overall, OCIO updated all its configuration management policy documents to align with existing practices. This resulted in the OCIO consistently executing its change management processes as outlined within its governing documents.

Although OCIO made improvements to its configuration management program, Williams Adley identified the following two (2) issues; one at the entity level and one at the system level:

Entity-level

(1) Performance metrics associated with SI's Configuration Management (CM) program are not defined within their governing documents.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, outlines the generation of metrics related to security-focused configuration management (SecCM) so that analysis and consolidation of monitoring reports can generate metrics such as the percentage of systems that are implemented in accordance with their approved baselines, the percentage of IT products that are configured in accordance with the organizationally defined common secure configurations, or percentage of system changes that have been subjected to security impact analyses.

The *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, outlines a maturity model approach and states that in order to be defined as an effective program, an entity needs performance metrics to evaluate the effectiveness of configuration management policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Performance metrics used to evaluate SI's configuration management program are not defined within its governing documents as the OCIOhas not developed a process to determine the

effectiveness of its configuration management policies and procedures and make updates, as appropriate.

Without defined performance metrics and a process to consistently evaluate its configuration management program, OCIO cannot identify potential areas for improvement and determine whether the configuration management program is meeting their desired objectives.

(2) OCIO did not maintain complete documentation to demonstrate the review of the component inventories as a part of the periodic component inventory reviews.

According to Information Technology Technical Standard & Guideline IT-930-03, *Security Assessment and Authorization Version 1.2,* major System Owners/Information System Representatives and ISSOs will review and update the component inventories for their systems at least quarterly.

As a part of the FY 2020 audit, Williams Adley determined that documentation was not retained by OCIO to demonstrate the quarterly component inventory reviews performed throughout the audit period because the *SI Hardware and Software Component Inventory* document did not outline the documentation retention requirements.

Without proper documentation, OCIO may not be able to validate whether all gaps within system component inventories were resolved and if all IT System owners and SI Mission Sponsors verified their system component inventories within [redacted]

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.

Williams Adley determined that in FY 2020, the identity and access management domain operated at Level 3 (Consistently Implemented) maturity. Specifically, one (1) metric question was rated a Level 4 maturity, seven (7) metric questions were rated a Level 3 maturity, and one (1) metric questions was rated a Level 2 maturity.

Overall, OCIO took steps to improve and implement an identity and access management program by updating its policies and procedures, such as its IT Technical Note 930-TN37 *Securing IT Accounts*, 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.

Although OCIO made improvements to its identity and access management program, Williams Adley identified the following two (2) issues; one (1) at the entity level and one (1) at the system level:

Entity-level

(1) OCIO did not document procedures for separation of duties and ensure use of least privilege for privileged accounts.

According to NIST SP 800-53, AC-5, "Separation of Duties" states, "The organization a) separates [Assignment: organization-defined duties of individuals] b) documents separation of duties of individuals; and c) defines information system access authorizations to support separation of duties". Furthermore, NIST SP 800-53, AC-6, "Least Privilege" states "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions".

As a part of the FY 2020 audit, Williams Adley reviewed SI's identity and access management governing documents such as IT-930-02, *Security Controls Manual Version 4.3* and IT-930-TN37, *Securing IT Accounts* and determined that OCIO has not developed procedures to support the concepts of separation of duties and use of least privilege across all information systems. Specifically, how system owners ensure that:

- Mission functions and information system support functions are divided among different individuals and/or roles;
- Information system support functions are supported by different individuals;
- Security personnel administering access control functions do not also administer audit functions; and
- Processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.

Without clear guidance to manage incompatible access rights and ensure least privilege to information systems, there is a risk of potential abuse of authorized access privileges and privileged users performing both access control and audit functions. For example, as a part of the FY 2020 FISMA audit, Williams Adley determined that a privileged BAS[10] user was able to review their own access as a part of the BAS privilege user review.

Data Protection and Privacy

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

Williams Adley determined that in FY 2020, the data protection and privacy program operated at Level 4 (Managed and Measurable). Specifically, three (3) metric questions were rated a Level 4 maturity and two (2) metric questions were rated a Level 3 maturity.

[10] Building Automation System (BAS) manages secured support for the heating, ventilation, and air conditioning (HVAC) management of air circulation, temperature, and humidity controls to protect collections as well as the comfort of visitors and employees.

Overall, SI's Privacy Office has made significant improvements to their Data Protection and Privacy program. SI has obtained and reviewed quantitative and qualitative performance measures on the effectiveness of its privacy activities; updated data protection and privacy policies and procedures; and consistently implemented its program to support various activities including but not limited to monitoring inbound and outbound network traffic to ensure that all traffic passes through a web content filter that protects against phishing, and malware. In addition, the Privacy Office measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII and sPII.

Although the Privacy Office made improvements to its data protection and privacy program, Williams Adley identified the following entity level issue:

Entity-level

(1) The Privacy Office has not documented a process to conduct a privacy-specific tabletop exercise on at least an annual basis.

According to OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* The Senior Agency Official for Privacy (SAOP) shall periodically, but not less than annually, convene the agency's breach response team to hold a tabletop exercise. Furthermore, *SD 119 - Privacy Breach Policy* does not include the requirements to perform a periodic tabletop exercise with the breach response team.

As a part of the FY 2020 audit, Williams Adley confirmed that the Privacy Office has made the strategic decision to start performing tabletop exercises for its breach response plan with the first exercise performed on June 23, 2020. However, the SI's Privacy Office has not developed a documented process to support future tabletop exercises.

Without an established process to conduct tabletop exercises and evaluate lessons learned, SI personnel may not be aware of how to properly execute the breach response plan and may not be able to make improvements to the plan, as needed.

Security Training

A security training program helps ensure that personnel at all levels understand their information security responsibilities and how to properly use and protect agency 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.

Williams Adley determined that in FY 2020, the security training program operated at Level 4 (Managed and Measurable). Specifically, five (5) metric questions were rated a Level 4 maturity and one (1) metric question was rated a Level 3 maturity.

Overall, the OCIO improved the security training domain by tailoring its annual security awareness training, as a result of employee feedback and conducting internal reviews of all training to determine its appropriateness to SI's environment. The OCIO also consistently implemented its

organization-wide security awareness and training strategy and plan such as allocating sufficient resources to consistently carry out its security awareness and training responsibilities for the enterprise-wide Computer Security Awareness Training and role-based training.

Williams Adley identified an instance in which established compensating controls were followed to address failed preventative controls. Specifically, a Lawson user did not complete their security training within the required 30-day timeframe. As a result, SI's GRC tool automatically created a HEAT ticket and the user's access was disabled. Lawson access was reinstated once training was completed, and completion status was communicated to the help desk.

Lastly, OCIO conducted a skill gap assessment in FY 2020; however, Williams Adley determined that OCIO has not yet fully addressed its identified knowledge, skills, and abilities gaps through training or hiring of additional staff/contractors. The process followed to address the identified skill gaps will be evaluated in subsequent years.

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, which seeks to provide visibility into IT assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. Williams Adley determined that in FY 2020, the Detect function operated at Level 3 (Consistently Implemented), the same as FY 2019.

INFORMATION SECURITY CONTINUOUS MONITORING

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[11] 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.[12]

Williams Adley determined that in FY 2020, ISCM operated at Level 3 (Consistently Implemented). Specifically, four (4) metric questions were rated a Level 3 maturity and one (1) metric question was rated a Level 2 maturity.

Overall, the OCIO improved its ISCM program by implementing lessons learned from the data gathered through the development of its qualitative and quantitative performance measures on the performance of its ISCM program. Williams Adley determined that the tools and architecture specified in the ISCM strategy were in place and OCIO added several new monitoring tools in FY 2020 to assist in their data gathering activities. Williams Adley also determined that system-

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

[12] 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.

specific dashboards are used to manage threats using the alerts created in [redacted] Although, SI has identified dashboards in its strategy, Williams Adley identified the following entity level issue:

Entity Level

(1) OCIO has not finalized its qualitative and quantitative performance metrics to determine the effectiveness of its Information Security Continuous Monitoring policies and procedures and makes updates as appropriate.

NIST SP 800-137**,** *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* states that the monitoring strategy should be reviewed regularly for relevance and accuracy in reflecting organizational risk tolerances, correctness of measurements, applicability of metrics, and effectiveness in supporting risk management decisions.

The *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, outlines a maturity model approach and states that in order to be defined as an effective program, an entity needs performance metrics to evaluate the effectiveness of ISCM policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Performance metrics used to evaluate SI's ISCM program are not defined within its governing documents as OCIO has not developed a supporting process to determine the effectiveness of its ISCM policies and procedures and make updates, as appropriate.

Without defined performance metrics and a process to consistently evaluate its ISCM program, OCIO cannot identify potential areas for improvement and determine whether the ISCM program is meeting their desired objectives.

RESPOND

The Respond function, which is comprised of one (1) domain, incident response, supports an agency's ability to act when responding to a detected cybersecurity incident and to limit the incident's impact. As stated in OCIO Technical Standard and Guideline IT-930-04, *Information Technology Security Incident Management*, Version 1.0, information systems are subject to a range of security incidents that can have a serious impact on SI's ability to perform its mission. Effective incident response (IR) is important for rapidly detecting, limiting the effects of, and recovering from information technology (IT) security incidents. Successful IR requires careful planning, adequate resources, and good communication. Williams Adley determined that in FY2020, the Respond function operated at Level 3 (Consistently Implemented), an increase of one maturity level since FY 2019.

INCIDENT RESPONSE

OCIO Technical Standard and Guideline IT-930-04, *Information Technology Security Incident Management*, 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.

Williams Adley determined that in FY 2020, the incident response program operated at Level 3 (Consistently Implemented). Specifically, two (2) metric questions were rated a Level 4 maturity and five (5) metric questions were rated a Level 3 maturity.

Overall, OCIO made improvements such as the implementation of detection and prevention tools to support incident response activities and improved its process to automatically report security incidents to internal and external stakeholders through the Security Operations Center Incident Management tool within [redacted] ensuring all incidents are reported in a timely manner. [redacted] is used to collect and review automated alerts generated by [redacted] In addition, OCIO used automated tools and dashboards to determine escalated threats and possible cyberattacks. The effectiveness of the IR program is measured through [redacted] dashboards and ISCM metrics. Although the OCIO identified dashboards in its strategy, the OCIO is currently in progress of defining and analyzing qualitative and quantitative performance measures to determine the effectiveness of its incident response policies and procedures and makes updates as appropriate. Williams Adley identified the following entity level issue:

Entity Level

(1) OCIO has not finalized its qualitative and quantitative performance measures to determine the effectiveness of its Incident Response policies and procedures and makes updates as appropriate.

NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide,* states that the IR plan should lay out the necessary resources and management support. The IR plan should include the elements such as metrics for measuring the incident response capability and its effectiveness.

The *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, outlines a maturity model approach and states that in order to be defined as an effective program, an entity needs performance metrics to evaluate the effectiveness of IR policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Performance metrics used to evaluate SI's IR program are not defined within its governing documents as the OCIO has not developed a supporting process to determine the effectiveness of its IR policies and procedures and make updates, as appropriate.

Without defined performance metrics and a process to consistently evaluate its IR program, the OCIO cannot identify potential areas for improvement and determine whether the IR program is meeting their desired objectives.

RECOVER

The Recover function seeks to reduce the negative impact of an information security event through the timely recovery of normal operations and is comprised one (1) domain, contingency planning.

Williams Adley determined that in FY 2020, the Recover function operated at Level 3 (Consistently Implemented), an increase of one maturity level FY 2019.

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 FY 2020, SI's contingency planning program operated at Level 3 (Consistently Implemented). Specifically, all seven (7) metric questions were rated a Level 3 maturity.

Overall, in FY 2020, SI made improvements including, the OCIO conducting an enterprise-wide [redacted] completing a system-level BIA. OCIO also ensured that each system owner used the results of a system-specific BIA for Disaster Recovery (DR) planning and conducting the annual disaster recovery plan test for all in-scope systems.

Williams Adley noted that the SI OCIO is currently in progress of defining and analyzing qualitative and quantitative performance measures to determine the effectiveness of its contingency planning policies and procedures and makes updates as appropriate. Williams Adley identified the following entity level issue:

Entity Level

(1) OCIO has not yet finalized its qualitative and quantitative performance metrics to determine the effectiveness of its contingency planning policies and procedures and makes updates as appropriate.

NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems Contingency Planning Guide for Federal Information Systems,* states that although contingency planning is associated with activities occurring in the Operation/Maintenance phase, contingency measures should be identified and integrated into all phases of the System Development Lifecycle (SDLC). Incorporating contingency planning into the SDLC reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented.

The *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 4.0, outlines a maturity model approach and states that to be defined as an effective program, an entity needs performance metrics to evaluate the effectiveness of contingency planning policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Performance metrics used to evaluate SI's contingency planning program are not defined within its governing documents as the OCIO has not developed a supporting process to determine the effectiveness of its contingency planning policies and procedures and make updates, as appropriate.

Without defined performance metrics and a process to consistently evaluate its contingency planning program, the OCIO cannot identify potential areas for improvement and determine whether the contingency planning program is meeting their desired objectives.

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 the Smithsonian Institution has made improvements in four (4) of five (5) functions but only one (1) meets the information security goals identified by Department of Homeland Security to achieve an effective information security program.

Williams Adley has developed three (3) recommendations to address the gaps identified within governing documents supporting the risk management, configuration management, and identity and access management programs:

Table 2: Governing Document Related Recommendations

Condition Identified	FISMA Domain	Recommendation #
OCIO did not maintain complete documentation to demonstrate the execution of its annual IT systems inventory review.	Risk Management	Recommendation #1
OCIO did not maintain complete documentation to demonstrate the review of the periodic component inventory reviews.	Configuration Management	
OCIO did not document procedures for separation of duties and ensure use of least privilege for privileged accounts.	Identity and Access Management	Recommendation #3
The Privacy Office has not documented a process to conduct a privacy-specific tabletop exercise on at least an annual basis.	Data Protection and Privacy	Recommendation #5

Williams Adley has developed one (1) recommendation to address control deficiencies within the risk management program:

Table 3: Control Deficiency Related Recommendations

Condition Identified	FISMA Domain	Recommendation #
IT-930-03, Security Assessment and Authorization Version 1.2, does not properly indicate where complete hardware and software records for each information system are located.	Risk Management	Recommendation #4

Williams Adley has developed one (1) recommendation to address the missing performance metrics within the configuration management, incident response, ISCM, and contingency planning programs and assist OCIO with meeting the requirements to be defined as effective under the FISMA maturity model:

Table 4: Performance Metric Related Recommendation

Condition Identified	FISMA Domain	Recommendation #
Performance metrics associated with SI's CM program are not defined within their governing documents.	Configuration Management	Recommendation #2
OCIO has not finalized its qualitative and quantitative performance metrics to determine the effectiveness of its ISCM policies and procedures and makes updates, as appropriate.	ISCM	
OCIO has not finalized its qualitative and quantitative performance measures to determine the effectiveness of its incident response policies and procedures and makes updates, as appropriate.	Incident Response	
OCIO has not yet finalized its qualitative and quantitative performance metrics to determine the effectiveness of its contingency planning policies and procedures and	Contingency Planning	

makes updates, as appropriate.		

RECOMMENDATIONS

Williams Adley presents the following recommendations to assist the OCIO Chief Information Officer with enhancing the information security program:

Recommendation 1: Update the *Annual* [redacted] *IT Systems Inventory* and *SI Hardware and Software Component Inventory* documents to outline the documentation retention requirements for these inventories.

Recommendation 2: For the information security program to be defined as effective under the FISMA maturity model, establish metrics and performance metrics to evaluate the effectiveness of configuration management, incident response, ISCM, and contingency planning policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Recommendation 3: Develop entity level procedures to ensure appropriate separation of duties and use of least privilege for privileged accounts. At a minimum, develop procedures to support the following processes:

- Periodic review and adjustment of privileged user accounts and permissions, and
- Inventorying and validating the scope and number of privileged accounts.

Recommendation 4: Update the *IT-930-03 - Security Assessment & Authorization document* to ensure that [redacted] is referenced instead of a documented system security plan to capture key system information, including but not limited to component inventories, security requirements, and security controls implementation details.

Williams Adley presents the following recommendation to assist the OCIO Chief Privacy Officer with enhancing the privacy program:

Recommendation 5: Update *SD 119 - Privacy Breach Policy* to include a process for conducting at least an annual tabletop exercise.

MANAGEMENT'S COMMENTS AND WILLIAMS ADLEY'S RESPONSE

OIG provided the Smithsonian Institution management with a draft of Williams Adley's report for review and comment. Management's response is presented in its entirety in Appendix F. Williams Adley did not audit management's response and, accordingly, do not express any assurance on it.

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.

General Criteria

a. Office of Management and Budget (OMB) Memorandum (M)-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*, November 19, 2019.

Risk Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.3*, Revision Date June 2020
b. SI Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization Version 1.2,* Revision Date June 2020
c. IT Security Procedure *Annual* [redacted] *IT Systems Inventory* Version 1.2, July 1, 2020
NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and System View,* March 2011
d. NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations,* December 2018
e. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Updated January 22, 2015
f. NIST SP 800-60 Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
g. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Security Systems,* February 2004

Configuration Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.3*, Revision Date June 2020
b. SI Technical Note IT-930-TN33, *Vulnerability Management Program*, Last Revised August 13, 2020
c. SI Technical Note IT-960-TN01, *Change Management*, Last Revised September 14, 2020
d. SI Technical Note IT-920-TN04, *Configuration Management*, March 29, 2019
e. SI Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization Version 1.2,* Revision Date June 2020
f. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Updated January 22, 2015
g. NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems,* August 2011 – Includes Updates as of October 10, 2019

Identity and Access Management

a. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Updated January 22, 2015
b. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security*

Controls Manual Version 4.3, Revision Date June 2020
c. SI Technical Note IT-930-TN37, *Securing IT Accounts,* June 22, 2020
d. SI Technical Note IT-960-TN12, *Active Directory Account and Password Requests,* November 2019
e. BAS Account Management Outline, Version 1.0
f. Lawson Access Control Procedure, May 21, 2020

Data Protection and Privacy

a. Smithsonian Directive 118, *Privacy Policy*, September 15, 2020
b. Smithsonian Directive 119, *Privacy Breach Policy*, September 12, 2018
c. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
d. OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* January 3, 2017

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 4.3*, Revision Date June 2020
c. SI Information Technology Technical Standards & Guidelines IT-930-03, *Security Assessment & Authorization Version 1.2,* Revision Date June 2020
d. SI Technical Note IT-930-TN33, *Vulnerability Management Program,* last revised August 13, 2020

Incident Response

a. SI Technical Standard and Guideline IT-930-04, *Information Technology Security Incident Management,* July 21, 2020

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. *BAS Contingency Plan & Disaster Recovery Plan,* Version 2.5, May 2020
d. *Infrastructure Disaster Recovery Plan "High Level Common Components,"* September 2020
e. *Lawson Disaster Recovery Plan,* Version 1, July 23, 2020

APPENDIX B – FISCAL YEAR 2020 CYBERSCOPE[13] REPORT

Overall	
FISMA Question	**FY2020 Assessment**
0.1 - Please provide an overall IG self-assessment rating (Effective/Not Effective).	Overall Level 3: Consistently Implemented – 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's (SI) General Support System (GSS) and two (2) out of 38 other major systems to perform detailed testing for the Fiscal Year (FY) 2020 Federal Information Security Modernization Act of 2014 (FISMA) audit. Overall, SI has made progress in addressing previously identified information security deficiencies and implementing its policies and procedures in all functions. In addition, SI has reauthorized all information systems in its environment. The SI Office of Chief Information Officer (OICIO) continues to conduct several initiatives to improve SI information security posture. Based on the assessment of SI's information security program, the overall maturity level is **Level 3: Consistently Implemented**. The Department of Homeland Security, Office of Management and Budget, and the Council of the Inspectors General on Integrity and Efficiency considers Level 4, Managed and Measurable, as an effective level at the metric, domain, function, and overall security program.

[13] CyberScope is a web-based application designed to gather and standardize data from federal agencies to support annual FISMA reporting.

Function: Identify – Risk Management	
FISMA Question	**FY2020 Assessment**
1 - To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including 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 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).	**Level 3: Consistently Implemented** –SI has defined a process to develop and maintain a comprehensive and accurate inventory systems and system interconnections. Furthermore, SI maintains a comprehensive inventory of its information systems.
2 - To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) 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 2020 CIO FISMA Metrics: 1.2, 1.3, 3.9, CSF: ID.AM-1).	**Level 3: Consistently Implemented** – SI has consistently utilized its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network and uses this taxonomy to inform which assets can/cannot be introduced into the network.
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 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?	**Level 3: Consistently Implemented** – SI has consistently utilized its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses utilized in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network.
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 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?	**Level 3: Consistently Implemented** – SI has categorized and communicated the importance/priority of information systems in enabling its missions and business functions. The importance/priority of the in-scope information systems evaluated as a part of the FY 2020 audit were considered in the execution of its various system level risk assessment processes.

5. To what extent has the organization 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, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?	**Level 3: Consistently Implemented** – SI has consistently implemented its governing documents (policies, procedures, and strategy) to support its various risk management activities. Furthermore, SI uses its risk profile to facilitate a determination of the aggregate level and types of risk that management is willing to assume. SI also consistently captures, and shares lessons learned on the effectiveness of risk management processes and activities to update the program.
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 (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; OMB M-15- 14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?	**Level 2: Defined** – SI has developed an information security architecture which outlines a defined process to: • Identify business requirements, derived from strategic and operational plans, that need to be met to support SI's mission; • Identify security requirements; • Identify target architecture; • Perform a gap analysis against SI's existing environment to identify which requirements were currently implemented or not fully implemented; and • Develop and implement a roadmap to remediate the requirement gaps identified.
7 - To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M19-03)?	**Level 3: Consistently Implemented –** SI individuals perform the risk management roles and responsibilities that have been defined across the agency.
8 - To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating	**Level 3: Consistently Implemented** – SI has consistently utilized POA&Ms to effectively mitigate security weaknesses.

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)?	
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 3: Consistently Implemented** – SI's system risk assessments are performed, and appropriate security controls are implemented on a consistent basis. SI utilizes the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities.
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-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)?	**Level 3: Consistently Implemented** – SI ensures that information about risks is communicated in a timely and consistent manner to all internal and external stakeholders with a need-to-know. Furthermore, SI actively shares information with partners to ensure that accurate, current information is being distributed and consumed.
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 of information) and SLAs are included in appropriate 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).	**Level 3: Consistently Implemented** – SI ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. SI obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance.
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	**Level 3: Consistently Implemented** – SI has implemented a GRC tool, [redacted] to provide a centralized view of risks across the entity's information systems.

activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?	
13 - Provide any additional information on the 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 from the questions above and based on all testing performed, is the risk management program effective.	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 3: Consistently Implemented**
Overall Function Maturity Level	**Level 3: Consistently Implemented**

Function: Protect – Configuration Management	
FISMA Question	**FY2020 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 3: Consistently Implemented** – SI individuals are performing configuration management roles and responsibilities that have been defined across the agency.
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** – SI has developed an organization wide configuration management plan that includes the necessary components. In addition, SI has developed system configuration management plans for the two (2) sampled in-scope systems.
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** – SI has developed, documented, and disseminated 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.

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 2020 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?	**Level 3: Consistently Implemented** – SI has consistently recorded, implements, and maintains under configuration control, baseline configurations of its information systems and an inventory of related components in accordance with the organization's policies and procedures.
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, RA-5, and SI-2; NIST SP 800- 70, Rev. 4, FY 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?	**Level 3: Consistently Implemented** – SI has consistently implemented, assessed, and maintained secure configuration settings for its information systems based on least functionality. SI has consistently utilized scanning capabilities against all systems on the network to assess and manage both code-based and configuration-based vulnerabilities.
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, RA5, SI-2, and SI-3; NIST SP 800- 40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?	**Level 4: Managed and Measurable** – SI centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe.
20 - To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26).	**Level 3: Consistently Implemented** – SI has chosen not to implement TIC as it is not applicable to their environment. However, SI has documented the measures to protect its network by utilizing [redacted].
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 decisions; implementation of approved configuration changes; retaining	**Level 2: Defined** – SI has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address, at a minimum, the necessary configuration change control related activities.

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, CM-3 and CM4; CSF: PR.IP-3).	
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.	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 3: Consistently Implemented**

Function: Protect – Identity & Access Management	
FISMA Question	**FY2020 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; NIST SP 800-63- 3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?	**Level 3: Consistently Implemented** – SI has defined roles and responsibilities for identity and access management and has developed an ICAM governance structure to align and consolidate SI's ICAM investments, monitoring programs, and ensuring awareness and understanding for all stakeholders. Additionally, SI 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, OMB M-19-17)?	**Level 3: Consistently Implemented** – SI is not subject to FISCAM; however, SI has consistently implemented its plan, policies, and procedures to support its Identity Management program at the enterprise and information system levels.
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; OMB M-19-17, 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** – SI has developed, documented, and disseminated its policies and procedures for Identity Management. Policies and procedures have been tailored to the SI's environment and include specific requirements.

26 - To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel 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, OMB M-19-17)?	**Level 3: Consistently Implemented** – SI ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened periodically.
27 - To what extent does the organization ensure that access agreements, including nondisclosure 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)?	**Level 4: Managed and Measurable** – SI uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.
28 - To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, and IA-8; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2020 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, NIST SP 800-157, and Cybersecurity Sprint)?	**Level 3: Consistently Implemented** – SI has implemented [redacted] for its information systems. Additionally, SI assessed and established password complexity guidelines in accordance with NIST recommendations. [redacted] are required for access to facilities.
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, 800-157; OMB M-19- 17, FY 2020 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?	**Level 3: Consistently Implemented** – SI has implemented a strong administrative authentication to protect systems using [redacted].
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 user accounts and permissions,	**Level 3: Consistently Implemented** – SI ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. SI [redacted]

inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2020 CIO FISMA Metrics: 2.3, 2.5, and 2.6; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; CSIP; DHS ED 19-01; CSF: PR.AC-4)	[redacted].
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-11, AC-12, AC-17, AC19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2020 CIO FISMA Metrics: 2.10 and 2.11.	**Level 3: Consistently Implemented** – SI ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), [redacted].
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?	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 3: Consistently Implemented**

Function: Protect – Data Protection and Privacy	
FISMA Question	**FY2020 Assessment**
33 - To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-20- 04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2019 SAOP FISMA metrics, Sections 1 and 2)?	**Level 4: Managed and Measurable** – SI conducts quantitative and qualitative performance measures on the effectiveness of its privacy activities and uses that information to make needed adjustments. SI also conducts an independent review of its privacy program and makes necessary improvements.
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	**Level 3: Consistently Implemented** – SI has consistently implemented policies and procedures for the specified areas, including(i) use of FIPS-validated encryption of PII and other agency sensitive data, as

REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2020 CIO FISMA Metrics: 2.8, 2.12; 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*	appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.
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 2020 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?	**Level 3: Consistently Implemented** – SI has consistently monitored inbound and outbound network traffic, [redacted].
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 2019 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?	**Level 4: Managed and Measurable** – SI monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate. SI ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.
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, FY 2019 SAOP FISMA Metrics, Sections 9 10, and 11)? (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 4: Managed and Measurable** – SI measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, SI made updates to its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing.
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.	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 4: Managed and Measurable**

Function: Protect – Security Training	
FISMA Question	**FY2020 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 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: AT-1; and NIST SP 800-50).	**Level 4: Managed and Measurable** – SI resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.
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: 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 3: Consistently Implemented** – SI has assessed the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, SI periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating SI's awareness and training strategy/plans.
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.	**Level 4: Managed and Measurable** – SI monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans and ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.
42 - To what degree have security awareness and specialized security training policies and procedures been defined and	**Level 4: Managed and Measurable** – SI has monitored and analyzed qualitative and quantitative performance measures on the effectiveness of

implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).	its security awareness and training policies and procedures. SI also ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format.
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 2020 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** – SI measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.
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 4: Managed and Measurable** – SI obtains feedback on its security training content and makes updates to its program, as appropriate. In addition, SI measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate.
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?	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 4: Managed and Measurable**
Overall Function Maturity Level	**Level 4: Managed and Measurable**

Function: Detect – Information Security Continuous Monitoring	
FISMA Question	**FY2020 Assessment**
46 - To what extent does the organization utilize an ISCM strategy that addresses ISCM requirements and activities at each	**Level 3: Consistently Implementing** – SI's ISCM strategy is consistently implemented at the organization, business process, and

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)?	information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. SI also consistently captures lessons learned to make improvements to the ISCM strategy.
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; 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)?	**Level 3: Consistently Implemented** – SI's ISCM policies and procedures are consistently implemented for the specified areas. SI also consistently captures lessons learned to make improvements to the ISCM policies and procedures.
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.	**Level 3: Consistently Implemented** – SI has defined ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies. SI has allocated budget to IT security.
49 - How mature are the organization's processes for performing ongoing assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls (OMB A-130, 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); NIST SP 800-18, Rev. 1, NISTIR 8011; OMB M-14-03; OMB M-19-03).	**Level 3: Consistently Implemented** – SI has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture.
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 –** SI has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, SI has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities.

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?	Williams Adley did not identify any additional processes not noted in the questions above.
Calculated Domain Maturity Level	**Level 3: Consistently Implemented**
Overall Function Maturity Level	**Level 3: Consistently Implemented**

Function: Respond – Incident Response	
FISMA Question	**FY2020 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 M19-03; FY 2020 CIO FISMA Metrics, Section 4; CSF: RS.RP1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).	**Level 3: Consistently Implemented** – SI has consistently implemented its incident response policies, procedures, plans, and strategies. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident response policies, procedures, strategy, and processes to update the program.
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-20-04; FY 2020 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?	**Level 4: Managed and Measurable** – SI's resources (people, processes, and technology) are allocated in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively.
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-20-04; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS8; and US-CERT Incident Response Guidelines).	**Level 3: Consistently Implemented** – SI has consistently utilized its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes precursors and indicators generated by, for example, the following technologies: [redacted].

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 3: Consistently Implemented** – SI has consistently implemented its containment strategies, incident eradication processes, processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations.
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: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)?	**Level 4: Managed and Measurable** – Incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.
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-20-04; PPD-41).	**Level 3: Consistently Implemented** – SI is not required to have a contract with DHS for Einstein implementation. SI has a contract with [redacted] 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 SI.
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* • *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)*	**Level 3: Consistently Implemented**– SI has utilized incident response tools including email anti-malware and host based anti-malware to support the incident response program. SI has implemented the tools to support incident response activities to include- [redacted].
59 - Provide any additional information on the effectiveness (positive or negative) of the organization's incident response	Williams Adley did not identify any additional processes not noted in the questions above.

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

Function: Recover – Contingency Planning	
FISMA Question	**FY2020 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 –** SI individuals are performing the disaster recovery roles and responsibilities that have been defined across the agency.
61 - To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and 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, FY 2020 CIO FISMA Metrics, Section 5).	**Level 3: Consistently Implemented –** SI has consistently implemented its defined information system contingency planning policies, procedures, and strategies. In addition, SI consistently implements technical contingency planning considerations for specific types of systems, including but not limited to methods such as server clustering and disk mirroring. Further, SI is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy, and processes to update the program.
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-19- 03; FY 2020 CIO FISMA Metrics, Section 5; CSF:ID.RA4)?	**Level 3: Consistently Implemented** – SI incorporates the results of organizational and system level BIAs into strategy and plan development efforts consistently. System level BIAs are integrated with the organizational level BIA.
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 2020 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?	**Level 3: Consistently Implemented** – SI information system contingency plans are consistently developed and implemented for the in-scope systems as appropriate and include organizational and system level considerations for the following phases: activation and notification, recovery, and reconstitution. In addition, system level contingency planning development/maintenance activities are integrated with other

	continuity areas including organization and business process continuity, disaster recovery planning, incident management, insider threat implementation plan (as appropriate), and occupant emergency plans.
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 2020 CIO FISMA Metrics, Section 5; CSF: ID.SC5 and CSF: PR.IP-10)?	**Level 3: Consistently Implemented –** SI has implemented processes for information system contingency plan testing and exercises. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/BCP.
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 2020 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?	**Level 3: Consistently Implemented –** SI consistently implements its processes, strategies, 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 organization'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. In addition, the SI ensures that alternate processing and storage facilities are configured with information security safeguards equivalent to those of the primary site. Furthermore, 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 3: Consistently Implemented** – SI 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. Two (2) of two (2) selected in- scope information systems, conducted annual contingency plan testing in FY 2020, as required.
67 - Provide any additional information on the 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	Williams Adley did not identify any additional processes not noted in the questions above.

above and based on all testing performed, is the contingency program effective?	
Calculated Domain Maturity Level	**Level 3: Consistently Implemented**
Overall Function Maturity Level	**Level 3: Consistently Implemented**

APPENDIX C – SYSTEM DESCRIPTIONS

Williams Adley presents the following information on each of the three systems that were evaluated as part of the FY 2020 Information Security Program Review:

- **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.
- **Building Automation System (BAS) -** BAS manages secured support for the heating, ventilation, and air conditioning (HVAC) management of air circulation, temperature, and humidity controls to protect collections as well as the comfort of visitors and employees.
- **Lawson** - Lawson is an accounting software which consists of the following modules: Accounts Payable, General Ledger, Asset Management, and Activity Management. Lawson is used to generate financial statements, pay non-merchandise vendors, and track expenses.

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."[14] 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 17, 2020, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency released the "FY2020 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 4.0." 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

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

configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, 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 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 test system contingency plans thoroughly and effectively; 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

BAS	Building Automation System
BIA	Business Impact Analysis
CCB	Change Control Board
CM	Configuration Management
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	Department of Homeland Security
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
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Directive
SD	Smithsonian Directive
SI	Smithsonian Institution
SIEM	Security Information and Event Management
SINet	Smithsonian Institution Network
SLA	Service Level Agreement
SP	Special Publication
sPII	Sensitive Personally Identifiable Information
SSP	System Security Plan
TIC	Trusted Internet Connection
US-CERT	United States Computer Emergency Readiness Team

APPENDIX F – MANAGEMENT'S COMMENTS

Smithsonian Institution

Office of the Chief Information Officer

Date: June 7, 2021 Deron Burba

To: Cathy L. Helm, Inspector General

CC: Douglas Hall, Acting Under Secretary for Administration
Allison Willcox, Acting Deputy Under Secretary for Administration
Janice Lambert, Chief Financial Officer
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
Grace Clark, Smithsonian Enterprises Chief Information Officer
Sandi Cheski, System Owner, Lawson
David McCauley, System Owner, Building Automation System
Stone Kelly, Office of Planning, Management and Budget

Subject: Management Response to *"Information Security: Fiscal Year 2020 Evaluation of the Smithsonian Institution's Information Security Program"*

Thank you for the opportunity to comment on the report. Management concurs with the recommendations and has already taken action to begin implementing them.

[redacted] **and Software Component Inventory documents to outline the documentation retention requirements for these inventories.**

Management concurs with this finding. OCIO has updated the *Annual IT Systems Inventory*

document, including the system inventory review procedures and roles and responsibilities. OCIO also updated *IT-930-03, System Security Assessment & Authorization* to clarify the requirements and relationship between the system component inventory records in [redacted] and the operational component inventory records covered by the *SI Hardware and Software Inventories* document. Management considers this recommendation completed.

Recommendation 2: For the information security program to be defined as effective under the FISMA maturity model, establish metrics and performance metrics to evaluate the effectiveness of configuration management, incident response, ISCM, and contingency planning policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

Management concurs with this finding. OCIO has defined a set of Key Performance Indicators (KPIs) to provide qualitative and quantitative measurements of the effectiveness of the processes covered by the FISMA metrics. We have developed an application within [redacted] to track measurements and corrective actions for these KPIs. We have also begun to record data for these KPIs but need additional time to ensure we have collected sufficient KPI measurements to close this recommendation. Management expects the remaining work to be completed by September 30, 2021.

Recommendation 3: Develop entity level procedures to ensure appropriate separation of duties and use of least privilege for privileged accounts. At a minimum, develop procedures to support the following processes:

- **Periodic review and adjustment of privileged user accounts and permissions, and**
- **Inventorying and validating the scope and number of privileged accounts.**

Management concurs with this finding. OCIO will update procedure documentation to include appropriate separation of duties and least privilege for privileged accounts. Additionally, BAS has revised their privileged account review procedures to ensure separation of duties and address the observation noted in the report. Management expects the remaining work to be completed by September 30, 2021.

Recommendation 4: Update the IT-930-03 - Security Assessment & Authorization document to ensure that [redacted] is referenced instead of a documented system security plan to capture key system information, including but not limited to component inventories, security requirements, and security controls implementation details.

Management concurs with this finding. OCIO has updated and clarified *IT-930-03, System Security Assessment & Authorization* [redacted]
Security Plan documents for capturing and referencing key system security information. Management considers this recommendation completed.

Recommendation 5: Update SD 119 - Privacy Breach Policy to include a process for

conducting at least an annual tabletop exercise.

Management concurs with this finding. The Smithsonian Privacy Officer coordinated with the Smithsonian's Directives Review Council to revise Smithsonian Directive (SD) 119, *Privacy Breach Policy,* and the associated Appendix, *Privacy Breach Reporting and Notification Process,* to include a process for conducting a tabletop exercise at least annually with the Smithsonian Privacy Council. The revised SD and Appendix were posted on Prism, the Smithsonian's intranet, on April 20, 2021. Management considers this recommendation completed.

For the recommendations that Management considers completed, evidence has been placed in the IG Evidence share.