In Brief

Fiscal Year 2018 Independent Evaluation of the Smithsonian Institution's Information Security Program

Report Number OIG-A-19-07, September 23, 2019

What OIG Did

The Office of the Inspector General contracted with Williams Adley to conduct this audit. The objective of the audit was to evaluate the effectiveness of the Smithsonian's information security program in fiscal year 2018.

Background

Each year, the Department of Homeland Security and the Office of Management and Budget publish metrics to assist inspectors general in their annual information security program assessments under the Federal Information Security Modernization Act. The metrics rank the maturity level of five cybersecurity functions on a scale of 1 to 5.

As an entity 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 2018, Williams, Adley & Company - DC, LLP (Williams Adley) found that the Smithsonian Institution (Smithsonian) made progress in maturing its information security program. Significant improvements included updating key policies like incident response and disaster recovery, implementing a security information and event management tool, conducting phishing training for staff, and standardizing the information collected for hardware and software. Overall, both the Identify function and Recover function progressed from Level 1: Ad-Hoc in fiscal year 2017 to Level 2: Defined in fiscal year 2018. The remaining three functions—Protect, Detect, and Respond—continued to operate at Level 2: Defined. The improvements led Williams Adley to assess the overall program maturity as Level 2: Defined for fiscal year 2018. However, the Smithsonian did not reach maturity Level 4: Managed and Measured, the level defined by the Department of Homeland Security as fully effective.

Williams Adley found that the Smithsonian's information security program was hampered because many of the information systems had not yet been reauthorized for use through a revised security review process. Until that process is complete, it will be difficult for the Smithsonian to monitor how well its IT security program manages security risks. Williams Adley also found that five of seven systems tested had not undergone a privacy impact analysis to assess the sensitive information stored in the system.

In addition, Williams Adley found that the Office of the Chief Information Officer (OCIO) continued to address existing issues that impacted the maturity of the information security program. As of fiscal year end 2018, OCIO was in phase three of a four-phase plan to implement its information security continuous monitoring strategy. OCIO was also working to define an information security architecture to align the information security program with the Smithsonian's business needs. OCIO was targeting July 2019 to define the architecture, so it was not in place before the end of fiscal year 2018.

What Was Recommended

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

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

OFFICE OF THE
INSPECTOR GENERAL

Smithsonian

Memo

Date: September 23, 2019

To: Lonnie Bunch, Secretary

Cc: Mike McCarthy, Acting Chief Operating Officer and Under Secretary for Finance and Administration
Greg Bettwy, Chief of Staff, Office of the Secretary
Deron Burba, Chief Information Officer
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Carmen Iannacone, Chief Technology Officer, Office of the Chief Information Officer (OCIO)
Danee Gains Adams, Privacy Officer, OCIO
Juliette Sheppard, Director, Information Technology Security, OCIO
Jeanne O'Toole, Director, Office of Protection Services
Douglas Hall, Deputy Director, Physical Security and Business Operations, Office of Protection Services
Curtis Lutz, Director HR & Admin Systems Division, OCIO
Frederica Adelman, Director, Smithsonian Associates
Kevin Holmes, Supervisory IT Specialist, Smithsonian Associates

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

Subject: Fiscal Year 2018 Evaluation of the Smithsonian Institution's Information Security Program (OIG-A-19-07)

This memorandum transmits the final report of Williams, Adley & Company - DC, LLP's (Williams Adley) on the fiscal year 2018 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 2018, 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. Management concurred with all nine 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 provided by Smithsonian managers and staff to Williams Adley and this office 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 2018

September 20, 2019

WILLIAMS ADLEY

Contents

WILLIAMS ADLEY

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

Dear Ms. Helm:

We are pleased to provide our report for the performance audit we conducted to evaluate the effectiveness of the Smithsonian Institution's (SI) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for the fiscal year ending September 30, 2018.

The report details the results of our evaluation of SI's information security program and practices. FISMA requires each agency Inspector General, or an independent external auditor, to conduct annual evaluations 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-18-02 (*"Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements"*) provides instructions for meeting this year's reporting requirements.

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

SI management has provided us with a response to this FY 2018 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. We appreciate the opportunity to assist your organization with this evaluation. Should you have any questions, please call Tony Wang, Partner, at (202)-371-1397.

Williams, Adley & Company-DC, LLP

September 20, 2019

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

Abbreviations

CCB	Change Control Board
CDM	Continuous Diagnostics Mitigation
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	United States Department of Homeland Security
DRP	Disaster Recovery Plan
ERP	Enterprise Resource Planning
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk and Compliance
HDC	Herndon Data Center
HRMS	Human Resource Management System
ICAM	Identity, Credential, and Access Management
IDMS	Identity Management System
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISSO	Information Systems Security Officer
IT	Information Technology
ITSS	IT Security Staff
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPS	Office of Protection Services
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Direction
PSCMS	Personnel Security Case Management System
PTA	Privacy Threshold Analysis
SD	Smithsonian Directive
SE	Smithsonian Enterprise
SI	Smithsonian Institution
SIEM	Security Information and Event Management
SINet	Smithsonian Institution Network
SMS	Security Management System
SP	Special Publication

SPIA	Smithsonian Privacy Impact Analysis
sPII	Sensitive Personally Identifiable Information
SPO	Smithsonian Privacy Office
SWH	Software House
TIC	Trusted Internet Connection
TRB	Technical Review Board
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Introduction

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

The fiscal year (FY) 2018 FISMA CyberScope metrics consist of five cybersecurity framework security functions: Identify, Protect, Detect, Respond, and Recover. These five functions comprise eight domains: Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning. The Department of Homeland Security (DHS) uses the FISMA CyberScope metrics to determine the maturity level of an entity's information security program. The maturity levels range from Level 1: Ad-hoc to Level 5: Optimized.

Purpose

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

Objectives, Scope, and Methodology

I. Objective

The objective was to conduct an independent review of the effectiveness of SI's information security program and practices covering the period October 1, 2017, to September 30, 2018 (FY2018).

II. Scope and Methodology

An independent assessment by Williams Adley of SI's IT security posture for programs and practices included testing the effectiveness of security controls for seven sampled SI systems. SI management assessed and categorized each of the seven systems as "moderate" using the Standards for Security Categorization of Federal Information and Information Systems (Federal Information Processing Standards [FIPS] Publication 199).[1] SI does not currently have systems in the "high" category; thus, "moderate" is the highest security category for systems in use at SI. Per FIPS 199, the unauthorized disclosure, modification, destruction, or disruption of access to a "moderate" category system would have a serious adverse effect on SI's operations, assets, and stakeholders.

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

Williams Adley assessed the following seven SI systems:

- Smithsonian Institution Network (SINet) – SI's General Support System (GSS), which includes network transports, network security, and shared infrastructure that provides the core capability to the remainder of SI's major applications and miscellaneous IT systems
- Identity Management System (IDMS) – SI Office of Protection Services (OPS) system used for background investigations and identity proofing with a biometrics data management system with a direct link to the Office of Personnel Management (OPM)
- Personnel Security Case Management System (PSCMS) – OPS system that handles critical personnel security functions, such as providing the results of background investigations
- Security Management System(s) (SMS) – OPS system that manages electronic security within SI's physical structure, including managing physical access to SI buildings and locations using badges
- ePMX – System that facilitates the IT procurement process for Smithsonian Enterprises (SE)
- Human Resource Management System (HRMS) – System that stores and processes personnel data on each employee
- TSA Tessitura – System that facilitates customer relationship management and event management

The systems selected for testing are rotated annually among the approximately 44 major IT systems. Of the seven sampled systems, two systems—SINet and IDMS—were fully assessed using all five FISMA security functions. The additional five system assessments were limited in scope to two FISMA security functions: Protect and Respond. For details on the seven systems, see Appendix C.

The SI OIG contracted Williams Adley to assess the effectiveness of SI's information security program and practices. Williams Adley performed the review from July 2018 through October 2018 in accordance with Generally Accepted Government Auditing Standards (GAGAS). GAGAS requires that Williams Adley plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the review objectives. Williams Adley believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the review objectives.

To perform this review, Williams Adley interviewed SI management, employees, and contractors to evaluate the effectiveness of SI's information security program in accordance with SI, National Institute of Standards and Technology (NIST), and Office of Management and Budget (OMB) guidance. Williams Adley also observed daily operations, conducted sampling based on expert judgment where applicable, inspected SI policies and procedures to supplement observations and interviews, and obtained sufficient evidence to support the conclusions and recommendations. Where possible, Williams Adley also reviewed system-generated outputs to support the conclusions.

For the FY2018 review, Williams Adley used the Inspector General (IG) FISMA CyberScope metrics to determine the status of SI's information security program. The FY2018 IG FISMA metrics consist of eight domains, grouped into five functional areas that correspond to the NIST

cybersecurity framework. A list and description of the five functional areas and eight domains is presented in Appendix D. The metrics rank the organization's maturity level on a scale of 1 to 5 using a series of 9–12 questions per level. See Table 1 for a description of each level and Appendix B for the detailed questions. Answers to each question were based on an assessment of both the entity-wide program and the seven systems selected for testing. To move from Level 1 to Level 2, the majority of metrics must be Level 2 or greater, unless they are not applicable to the entity. For example, SI decided not to implement personal identity verification (PIV) cards and a Trusted Internet Connection (TIC); therefore, the fact that PIV and TIC were not implemented in the SI environment was not considered when determining the maturity of SI's information security program. DHS considers an effective information security program to be Level 4: *Managed and Measurable*.

Table 1: Fiscal Year 2018 Maturity Model for FISMA Cybersecurity Functions

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

Note: The maturity levels range from Level 1: Ad-hoc to Level 5: Optimized. An effective cybersecurity function is Level 4: Managed and Measurable or above. If an entity achieves Level 4 in the majority of the five cybersecurity functions evaluated, its information security program is considered effective overall.

Source: FY2018 IG FISMA Metrics

Background

I. The Smithsonian Institution

Smithsonian Institution was established by an Act of Congress signed by President James K. Polk on August 10, 1846. SI is a trust instrumentality administered by a Board of Regents and a Secretary. Since its founding, SI has become one of the world's largest museum and research complexes, consisting of 19 museums, the National Zoological Park, and nine research facilities, libraries, and archives. A major portion of SI's operations is funded from federal appropriations. In addition to federal appropriations, SI receives private support, government grants and contracts, and income from investments and various business activities.

II. The Office of the Chief Information Officer

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

The OCIO has primary responsibility for setting IT security policy, managing SI's IT security program, and partnering with all units and system owners to evaluate IT system security for the approximately 44 major IT systems. The IT security group is managed by the Director of IT Security, who reports directly to the Chief Information Officer (CIO). SI does not have any systems with a security categorization of "high," but does have "moderate" and "low" systems as defined by FIPS 199.

III. Smithsonian Privacy Office

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

IV. Office of Protection Services

OPS ensures the safety and security of the staff, visitors, and National Collections of the Smithsonian Institution, while permitting an appropriate level of public access to collections and properties. OPS provides essential protection and physical security functions and services, security management, and criminal investigations for 19 museums, the National Zoo, and nine research facilities. OPS also manages SI's physical access to Smithsonian facilities. Systems operated by OPS include the IDMS, SMS, and PSCMS.

V. Federal Information Security Modernization Act of 2014

Through the Federal Information Security Management Act of 2002,[2] as amended by the Federal Information Security Modernization Act of 2014,[3] Congress recognized the importance of information security to the economic and national security interests of the United States. FISMA assigns specific responsibilities to executive branch agencies, NIST, OMB, and DHS to strengthen the security of information systems.

Annually, OMB, in coordination with DHS, provides guidance on reporting categories and questions for meeting the current fiscal year's reporting requirements.[4] OMB uses the data to carry out its oversight responsibilities and to prepare its annual report to Congress on the entity's compliance with FISMA. SI is not required to comply with FISMA because it is not an executive branch agency; however, SI applies FISMA standards as a best practice to the extent practicable and consistent with its mission. For details about FISMA domains and how they are scored, see Appendix D.

Results of Audit

I. 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.[5] The Identify function is composed of the risk management process, which includes ongoing information system authorization, and promotes the concept of near-real-time risk management at the entity, business unit, and information system levels.

In FY2018, the Identify function operated at Level 2: Defined because all information systems were going through the authorization to operate (ATO) process. Also, not all associated IT risks were centrally tracked in the automated governance, risk and compliance (GRC) tool because IT risks are identified throughout the authorization process. In addition, risk management policies and procedures were not fully implemented in three of the seven systems selected for testing.

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 mitigation strategies may not be implemented. Without fully understanding the complete environment, management may be unknowingly accepting an unacceptable level of risk.

In FY2018, the risk management program operated at Level 2: Defined. SI improved its risk management program by (1) implementing a process for using standard data elements and taxonomy to develop an up-to-date inventory of hardware and software assets connected to the organization's network; (2) categorizing and communicating the importance and priority of

[2] *E-Government Act of 2002*, Public Law 107-347, December 17, 2002.

[3] *Federal Information Security Modernization Act of 2014*, Public Law 113-283, December 18, 2014.

[4] OMB, *Fiscal Year 2017–2018 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-18-02, October 16, 2017.

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* February 2014.

information systems in enabling its missions and business functions; (3) defining the roles and responsibilities of stakeholders involved in risk management; and (4) communicating information security risks to all necessary internal and external stakeholders. SI also continued to work on implementation of an automated GRC tool and re-authorization of all 44 major systems.

The re-authorization requirement was identified in the FY2014 report, which OIG closed in FY2018 with the understanding that OCIO would continue to complete re-authorization by implementing a planned schedule.[6] Part of this process includes determining if all identified major systems are, in fact, major systems or if they need to be reclassified as minor systems. By the end of FY2018, SI completed the re-authorization process for 10 major systems, which is approximately 25% of the total re-authorization effort.

Entity-level

(1) OCIO had not completed documenting an information security architecture that aligned with the SI strategic plan.

At the end of FY2018, OCIO was still working to document an information security architecture, with a target date of July 31, 2019. Although the full architecture was not yet complete, OCIO documented and began implementing an information security continuous monitoring (ISCM) strategy, which is part of the overall architecture. An ISCM strategy helps mitigate some security risks through monitoring, but the information security architecture helps ensure that the security needs are aligned with business needs. If the information security needs are not aligned with the business needs, the most critical SI information resources may not be adequately protected.

(2) Not all information systems have completed re-authorization using the GRC tool.

NIST Special Publication (SP) 800-39*, Managing Information Security Risk; Organization, Mission, and Information System View*, states: "organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leaders/executives develop a better understanding of the ongoing risk to organizational operations and assets, individuals, other organizations, and the Nation." In FY2017, SI began implementing an automated GRC tool to provide a centralized view of risks across SI's information systems. However, by the end of FY2018, not all information systems had completed the re-authorization process, which includes entering associated security controls, risks, and plans of action and milestones (POA&Ms) into the automated GRC tool. Until all systems have been re-authorized, and the associated risks entered into the automated GRC tool, SI may not be able to monitor how well its information security program is managing IT security risks.

System-level

(3) The Identity Management System, which stores background check and fingerprint data, did not have a valid authorization to operate during FY2018 due to a delay in re-assessing its security under the revised assessment and authorization process.

OCIO's Technical Standard and Guideline IT-930-03, *Security Assessment and Authorization* requires that every IT system and its components undergo the Security Assessment and Authorization process to assess the risks of operating the system and to make an informed

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

decision that those risks are at an acceptable level for SI. The assessment and authorization process culminates in an official authorization to operate (ATO), which is issued for 1 to 3 years depending on the risk level of the system. When the ATO expires, the system must undergo the assessment and authorization process again to ensure that continued operation of the system does not present unacceptable risk to SI.

Williams Adley requested the ATO letters for 2 of 44 systems—IDMS and SINet—and determined that the ATO for IDMS expired in FY2017. For FY2018, Williams Adley confirmed that OPS was working with OCIO to re-authorize IDMS, with a target completion date in FY2019. IDMS collects and electronically transmits sensitive PII and fingerprint data to OPM and the Federal Bureau of Investigation for the purpose of conducting criminal history checks. While efforts were made to re-authorize IDMS, resource constraints and delays prevented completion of the re-authorization process. Without official authorization to operate IDMS, management is operating a system where security controls may not be up-to-date, policies and procedures may no longer be relevant or not aligned with SI security procedures, and current information security risks with IDMS may not be identified or tracked by OCIO management.

(4) OPS did not properly maintain up-to-date interconnection agreements with major external systems.

OCIO's Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, control CA-03, states that the system interconnection agreements should be updated "annually." SI has a memorandum of understanding and interconnection agreement in place with OPM for the security of the data transmission; however, Williams Adley determined that the agreements were last updated November 11, 2009. OCIO stated that it was in the process of reviewing agreements; however, no explanation was given on why they had not been updated during the last 8 years, considering that OPM had a major breach in 2015. Williams Adley did not test the interconnection between OPM and SI, but it is possible that a breach could affect the memorandum of understanding. OCIO management stated that there were key positions open, such as Information Systems Security Officer (ISSO), which remained unfilled throughout FY2018. If ISSOs are not consistently available to be responsible for such tasks as updating information system interconnection agreements, reviewing and updating information system controls, and providing implementation details for the information system controls, then OPS' risk management program efforts are hindered. Without up-to-date signed contracts, SI is at risk of transmitting and receiving background investigation details without the necessary security controls in place.

II. 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 domains: configuration management, identity and access management, data protection and privacy, and security training. Data protection and privacy, a new process, was added to the metrics in FY2018.

In FY2018, the Protect function operated at maturity Level 2: Defined, which reflects the Protect function's four domains. During FY2018, three domains—configuration management, identity and access management, and data protection and privacy—operated at Level 2: Defined. The security training domain operated at Level 3: Consistently Implemented. The configuration

management domain and the security training domain have improved by one maturity level since the FY2017 assessment.

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 making adjustments to 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's 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 necessary changes.

In FY2018, the configuration management domain operated at Level 2: Defined. SI took steps to improve its configuration management program by ensuring that hardware and software used at the entity level were appropriately documented and tracked in the automated GRC tool. By the end of FY2018, SI had not addressed the following configuration management issues.

Entity-level

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

OCIO's Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, control CM-01, states that the configuration management policy and procedures should be reviewed and updated "at least every 3 years." Williams Adley requested the current configuration management plan, policies, and procedures from OCIO. OCIO did provide Williams Adley with several technical notes[7] surrounding configuration management, but one of the documents provided—Technical Standard and Guideline IT-960-TN01, *Change Management*—was last updated August 8, 2013. In FY2018, per OCIO management, SI focused on implementing the automated GRC tool and ISCM strategy, and re-authorizing its information systems, leading to resource constraints for updating its configuration management plan. Without a comprehensive and up-to-date configuration management plan, SI cannot efficiently support its configuration management processes and enhance its critical infrastructure services to mitigate information security risks. Configuration errors also could introduce vulnerabilities to cyberattacks.

System-level

Based on Williams Adley's review, six of the seven sampled information systems had not completed the re-authorization process. The re-authorization process ensures that appropriate security controls have been properly updated and maintained for all information systems and that required policies and procedures have been implemented. Williams Adley found the following system-level deficiencies, which may have been prevented if the re-authorization process had been completed.

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

(2) The Change Control Board (CCB) could not verify that all sampled testing had been completed because change ticket assignees did not document test results for 9 of 22 configuration changes in the SINet system.

OCIO's Technical Standards & Guidelines IT-960-TN01, *Change Management*, states that if testing is completed, the testing process and results must be documented. Williams Adley requested the supporting documentation for 22 of the 4,886 documented changes, reviewed the supporting documents, and determined that 9 of the 22 changes did not have documentation in the change ticket showing the testing results, as required. The change ticket assignees noted that testing had been completed, but did not include the associated results as required. Without documentation of the testing results, the CCB would be unable to verify that testing had been completed appropriately.

(3) SINet's system owner did not keep an accurate list of hardware inventory.

According to Technical Standards & Guidelines IT-930-03, *Security Assessment & Authorization*,

> *The System Owner/System Owner Representative and ISSO are responsible for maintaining an inventory of all the hardware, software, and other components that are included within their system. System Owners/System Owner Representatives and ISSOs are responsible for ensuring that information related to their systems remains current.*

OCIO provided Williams Adley with the official hardware component inventory list for its data center. Using the inventory, Williams Adley conducted two different tests to verify that the inventory was accurate and complete. In the first test, Williams Adley selected 11 servers from the inventory and attempted to physically locate them at the data center, but was unable to locate 2 of the 11 servers selected. OCIO staff stated that some servers had been relocated recently and that the location had not been updated in the tracking system; OCIO was unable to provide an updated location. In the second test, Williams Adley selected 11 servers from the data center and traced them back to the component inventory. Without fully understanding the complete hardware inventory, including where devices are physically located, management may be hampered in responding to time-sensitive security issues.

(4) The TSA unit did not define roles and responsibilities in the Tessitura configuration management policies and the policies were not properly updated as required.

According to NIST 800-53 rev 4 control CM-1, "the organization develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance." Williams Adley requested the current configuration management plan, policies, and procedures for the Tessitura system. The document that was provided—*Policies & Procedures for Tessitura Support*—did not have defined roles and responsibilities. TSA management expressed the view that because there were so few employees in the unit, and because the requirement for each IT individual was transparent, there was no need to explicitly define roles and responsibilities in the policies. Without defined roles and responsibilities, Tessitura staff, especially new staff, may not be aware of their roles and responsibilities within the configuration management process.

(5) ePMX' system owner did not define responsibilities for configuration management personnel in the ePMX system's configuration management policies and procedures document.

OCIO's Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1* states that control CM-09 is required; however, the associated language detail was not provided. Therefore, Williams Adley used the supporting NIST 800-53 CM-09 control, which states,

> *The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.*

ePMX personnel provided Williams Adley with the ePMX system's configuration management policies and procedures document. Williams Adley determined that the document did not define the responsibilities of configuration management personnel as required. At the end of FY2018, ePMX was still going through the re-authorization steps, one of which was to ensure that policies and procedures are up-to-date and contain all the required information. Without identifying the responsibilities for configuration management personnel, there would be a lack of accountability for progressing through the configuration management processes.

(6) Four of seven sampled systems did not have documented policies and procedures for maintaining a complete and accurate software and hardware inventory.

According to Technical Standards & Guidelines IT-930-03, *Security Assessment & Authorization*,

> *The System Owner/System Owner Representative and ISSO are responsible for maintaining an inventory of all the hardware, software, and other components that are included within their system. System Owners/System Owner Representatives and ISSOs are responsible for ensuring that information related to their systems remains current. At minimum, the System Inventory and the Component Inventory will be updated under the following circumstances:*
> *• Smithsonian Units (including OCIO) will report new IT systems and significant changes to inventoried IT systems (including retirement of systems) to IT Security Staff (ITSS) within 60 days of the change*
> *• The system inventory will be updated as appropriate prior to Smithsonian Technical Review Board (TRB) final approval for any new/modified/replaced systems*
> *• System Owners will report the retirement of their systems to ITSS as part of the system retirement process. This includes termination of any contracted system*
> *• On an annual basis, ITSS will ask System Owners and Smithsonian Unit IT Managers to review the inventory of IT systems and provide any changes*
> *• System Owners/System Owner Representatives and ISSOs will review and update the component inventories for their systems at least annually*

Williams Adley requested the component inventory policies and procedures for the seven sampled systems to determine if there is a defined process on how to maintain a complete and accurate inventory of hardware and software components and software licenses used within the IT environment. Williams Adley was informed by the IDMS, Tessitura, ePMX, and PSCMS

owners that the systems did not have a defined process for maintaining a complete and accurate software and hardware inventory. Based on Williams Adley's inquiries, IDMS, Tessitura, ePMX, and PSCMS system owners did not know that IT-930-03, *Security Assessment & Authorization* requires system owners to update their configuration management policies and procedures to include the maintenance of system inventory at the system level. Without fully understanding the process of maintaining a software and hardware inventory, the individuals tasked with inventory maintenance may not be able to ensure completeness and accuracy.

(7) System owners for two of seven systems, HRMS and ePMX, did not maintain a complete list of hardware and software component inventories. System owners for the TSA Tessitura system did not maintain a complete software component inventory.

According to Technical Standards & Guidelines IT-930-03, *Security Assessment & Authorization*,

> *• On an annual basis, ITSS will ask System Owners and Smithsonian Unit IT Managers to review the inventory of IT systems and provide any changes*
> *• System Owners/System Owner Representatives and ISSOs will review and update the component inventories for their systems at least annually*

The SI Taxonomy Information document states that the following information should be captured for hardware and software assets: device name, Internet Protocol (IP) address, location, image name, software version, system contact, product type, last boot time, image type, image family, and serial number.

For HRMS, Williams Adley noted that only the names and descriptions of the servers were tracked, along with the associated software on the HRMS inventory list. The list did not provide a location, asset number, or owner, all of which are required to be included in a full hardware and software component inventory.

For ePMX, Williams Adley was provided with the ePMX list of hardware and software component inventories and determined that the hardware inventory list did not provide a location, asset number, or owner.

For TSA Tessitura, Williams Adley requested a complete list of component inventories, but the TSA Tessitura system owner did not provide Williams Adley with the software component inventory. Williams Adley made several attempts to collect the information, but as of the end of October 2018, the information had not been provided.

As stated above in (6) Four of seven sampled systems…, system owners did not have a procedure for tracking hardware and software and were not aware of their responsibility to track component details. Without fully understanding the complete hardware and software inventory, system owners may not be adequately protecting critical software and hardware, which increases the risks to the information that resides there.

(8) OCIO did not remedy high criticality security vulnerabilities in SINet within documented timelines.

According to Technical Standards & Guidelines IT-930-TN33, *Vulnerability Management Program*, Table 2 defines the following remediation requirements based on asset criticality for high vulnerabilities:

> *• High asset criticality – 2 weeks*

•*Very High asset criticality – 5 days*

Williams Adley compared November 2017, March 2018, and August 2018 vulnerability scan reports for the production SINet servers. Williams Adley determined that 572 high to very high vulnerabilities were identified in November 2017, and again identified in March 2018, and that 294 of those vulnerabilities were again identified in August 2018 (9 months later). High risk system vulnerabilities that remain unresolved provide a readily available avenue for hackers. OCIO management personnel stated that they are in the process of implementing new procedures to ensure that vulnerabilities are addressed in a timely manner, but the process was not completed as of FY2018.

Identity and Access Management

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

In FY2018, the Identity and Access Management process operated at Level 2: Defined. OCIO has defined policies and procedures, but not all system owners have ensured that user access authentication and user access provisioning were fully implemented across the organization.

Entity-level

(1) OCIO did not implement the NIST-recommended two-factor authentication for privileged users to access its facilities and networks.

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

Williams Adley's review found that OCIO required users to enter a security token and password to gain remote access to its internal computer network. However, the same strong authentication process was not implemented for users, including privileged users, to access SI networks and systems while onsite. Without strong authentication, less sophisticated cyber criminals or insiders could gain unauthorized access to SI's information and systems.

System-level

(2) 1 of 18 SINet user accounts tested for separation did not have an associated HEAT ticket and 1 of 22 new users tested did not have a signed Rules of Behavior form on file.

Technical Note IT-960-TN12, *Active Directory Account and Password Requests* states that "after an employee departs the Smithsonian Institution, the account is disabled. The only exception to this rule is when a former employee returns in a non-employee role." IT-960-TN12 also requires that all requests for change, addition, or deletion of an active directory account have a completed HEAT ticket. In addition, Smithsonian Directive (SD) 931, *Use of Computers,*

Telecommunications Devices and Networks requires all users who are to be granted an account on the SINet must agree to abide by Smithsonian acceptable usage policies. Users must sign this agreement to obtain a user account.

Williams Adley selected 18 SINet users that separated from SI during FY2018. Testing results identified one individual who did not have a HEAT ticket documented for the separation. Williams Adley requested the user's HEAT ticket associated with the separation, but it was not provided.

Williams Adley also tested 22 sampled SINet new users' access request HEAT tickets and found that one individual did not have a signed Rules of Behavior form on file. OCIO was unable to provide the signed user agreement form.

Williams Adley determined that SI did not properly manage user access for all new and separated users. If SI does not follow the proper management process, it may be unable to effectively reduce the risk of unauthorized access to sensitive information.

(3) SMS was unable to provide evidence that 13 of 13 user accounts selected for separation testing were properly separated.

Technical Note IT-960-TN12, *Active Directory Account and Password Requests* states that "after an employee departs the Smithsonian Institution, the account is disabled." To ensure that the individual's account is disabled, IT-960-TN12 requires that all requests for change, addition, or deletion of an active directory account have a completed HEAT ticket.

Williams Adley selected for testing 13 SMS user accounts for users who separated in FY2018. Williams Adley requested supporting evidence for the sampled accounts, but SMS was unable to provide HEAT tickets. If evidence for deactivation of SMS user accounts on separation is not maintained, SMS management may be unable to monitor the timely removal of accounts of separated SMS users, and may unknowingly allow a separated user to maintain access.

(4) SMS did not require or maintain proper access agreements for new users transferred from other units.

OPS Security Management System(s) IT Security (OPS-58) states that "all users of the OPS SMS must sign a password receipt and user responsibility agreement (User Account Form) before access to a SMS is permitted. User accounts for unit control operators and central control operators will be requested through the Unit Security Manager. All other user accounts for access to the OPS SMS are requested through the unit's TSD System Administrator."

Williams Adley, after reviewing the SMS *Password Receipt and User Responsibility Acknowledgement Building Level OPS SMS Client & Request for Access to the Building Level OPS SMS Client* forms, determined that SMS users were granted access in accordance with OPS policies and procedures. However, Williams Adley was not provided with the supporting user agreements for 10 of 22 sampled users who were granted access to SMS during FY2018. OPS management informed Williams Adley that it was an OPS management decision to allow all of the Unit Control Room Operators to be users in all control room systems to enable them to work in any unit control room. An evidential email was provided to Williams Adley wherein the OPS System Administrator was directed by the OPS Deputy Director to provide access to the operators. OPS explained that access to the SMS control rooms was granted to the control room operators without the required OPS SMS User Responsibility Acknowledgement forms because

the operators already had a signed user agreement with their original unit on hire. However, the OPS SMS-specific user agreement form is required to gain SMS access, per OPS-58. Without proper documentation, SMS would be unable to properly manage user access or determine if the access is appropriate based on the user's job responsibilities.

(5) One of three sampled privileged users did not complete a proper user agreement form and did not take required training before gaining access to PSCMS.

According to Technical Note IT-930-TN37, *Securing IT Accounts* all privileged users must "sign an Elevated Privileges Agreement prior to receiving administrative credentials. Existing personnel with administrative credentials must sign the agreement within 30 days of issuance." Additionally, "personnel with administrative privileges to any IT system must complete course S-111: Privileged User Security and sign an *Elevated Privileges Agreement*."

Williams Adley selected one of three PSCMS privileged users for testing. Based on a review of the sampled privileged user's *Elevated Privileges Agreement* and security training (S-111) certification, the user's last IT Admin login date was May 21, 2018, but the user agreement was signed October 3, 2018, and the S-111 certification was completed October 24, 2018. Williams Adley determined that neither the user agreement nor the training certification was completed within 30 days of the user obtaining a role as the PSCMS IT Administrator, as required. Because IT administrators have a major impact on the confidentiality, integrity, and availability of SI systems and information, it is essential that they understand their role in maintaining security. Maintaining security is even more critical for PSCMS because it houses SI's highly sensitive background check data. OCIO explained that the user was one of the individuals who helped implement the system and was not aware that they were required to complete the course. Additionally, the individual was not supporting the system full-time as an administrator.

(6) One of seven sampled systems did not periodically review user account activities for misuse, as required by OCIO policy.

According to Technical Note IT-930-TN37, *Securing IT Accounts*, "each system must have a documented process for managing accounts that includes: a process to periodically review accounts on at least a quarterly basis and modify or deactivate accounts as appropriate." Williams Adley requested the supporting evidence indicating that periodic reviews from Tessitura were conducted and documented, but TSA management did not provide any supporting documentation. During Williams Adley's inquiries with TSA management of their process of quarterly reviews, TSA management stated that although TSA did complete a review of accounts when summer interns departed in FY2018, there was no documentation of the review. If there is not proper logging and periodic review of user account activities, a misuse of privileged functions may not be detected.

Data Protection and Privacy

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

In FY2018, the Data Protection and Privacy program operated at Level 2: Defined. Williams Adley noted that SI did not update the supporting policies and procedures and did not fully

configure supporting tools for the Data Protection and Privacy program. Williams Adley also noted that continuous monitoring reports, the Privacy Threshold Analysis (PTA), and the Smithsonian Privacy Impact Analysis (SPIA), were not completed for five of seven systems tested. The PTA and SPIA are designed to assess the use of PII and/or sPII in the system to identify potential privacy risks and the need for mitigations.

Entity-level

(1) The Privacy Office did not maintain up-to-date privacy policies and procedures throughout FY2018.

Smithsonian Directive (SD), 118 *Privacy Policy* states that SD 118 must be reviewed at least every 2 years. Additionally, SD 119, *Privacy Breach Policy* states that it must be reviewed annually. The Smithsonian Privacy Office's (SPO) privacy program has a defined program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems. However, not all privacy policies and procedures were up-to-date throughout FY2018. Specifically, SD 118, *Privacy Policy* had not been updated since March 11, 2014, and the updated SD 119, *Privacy Breach Policy*, which was implemented June 24, 2010, was not finalized until September 12, 2018. SI had SD 119, *Privacy Breach Policy* in place for only 3 weeks of the audit period.

According to the Smithsonian Privacy Officer, SD 118 is on the list to be updated, but was not updated in FY2018 because efforts were focused on conducting a PII inventory of all information systems in use at the SI and on finalizing the SD 119 update in a timely manner. Without up-to-date guidance provided by the Data Protection and Privacy program, internal users may fail to comply with new laws and regulations, and without stakeholders' adequate awareness (e.g., what is considered a PII violation), PII could be mismanaged and improperly handled.

(2) OCIO did not properly configure data loss prevention tools to support the Data Protection and Privacy program.

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

Williams Adley found that OCIO had established rules for the data loss prevention (DLP) function in Office 365, which identifies possible data exfiltration but does not prevent it. However, because Office 365 was not implemented until the midpoint of FY2018, the DLP function found within Office 365 was not in place for all of FY2018. Per SPO's preparation of the Possible Office Exchange Online Data Loss Prevention Improvement document, the DLP tool that OCIO had in place since May 14, 2018 was configured to identify and alert OCIO personnel of possible leakage of sensitive information after the DLP policy is violated. OCIO is currently implementing new DLP rule sets. Once implemented, instead of OCIO being alerted after PII leakage has been detected, SI Microsoft Outlook will prompt users to enter a business justification before an email containing PII is sent, with the justifications being stored in the audit logs. Implementation of the new DLP should be completed in FY2019. Without a fully

configured DLP tool in place, OCIO would not be able to fully prevent sensitive information from being intentionally or unintentionally shared with outside parties.

(3) SI's privacy awareness training did not include all required components.

According to Smithsonian Directive (SD) 118, *Privacy Policy*,

> *All Staff and Affiliated Persons are required to complete annual Computer Security Awareness Training, which currently includes general information for handling and safeguarding Smithsonian data, including PII and sPII. The SPO shall develop, update and deliver additional privacy training and awareness programs to Units that use PII and sPII. Such training may be held in order to address compliance with this policy and/or, in conjunction with OCIO, to address security measures necessary to maintain the privacy of Smithsonian data.*

OCIO's Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, control IR-09(2) states that SI needs to "provide information spillage response training annually." The SPO's SD 119, *Privacy Breach Notification Policy,* and the associated Appendix, *Privacy Breach Reporting and Notification Process, Technical Note IT-930-TN30* and SD 309, *Merchant Accounts, Payment Cards and the Payment Card Industry (PCI) Data Security Standard*, states that all staff are responsible for reporting privacy and/or security incidents, including information spills, and for alerting the Security Operations Center, SPO, and members of the PCI Working Group. In addition, the *SINet System Security Plan* states that "the annual CSAT, ISAT and P101, targeted role-based trainings will address information spillage in future training materials."

Basic privacy awareness information, such as defining PII and sPII, is included in annual information security awareness training. In addition, the SPO identifies the roles that require individuals to handle PII as a regular part of their job responsibilities. The SPO requires individuals who handle PII to take *Privacy 101*, which presents more detailed privacy awareness training. Other individuals may voluntarily take *Privacy 101*, but it is not required. In FY2018, 9,764 individuals were required to take the general security awareness training; 2,004 individuals took *Privacy 101*.

Williams Adley's review of the basic security awareness training found that the training did not cover data collection requirements, the consequences of failing to properly handle PII, or how to handle information spillage. The first two items, data collection requirements and PII handling, are found in *Privacy 101* training. However, as stated above, *Privacy 101* training is not mandatory for all SI users. OCIO management stated that the lack of content related to information spillage was due to resource constraints, but recognized that it is an issue, stating the following in SINet's Security Plan, "the annual CSAT, ISAT and P101, targeted role-based trainings will address information spillage in future training materials." Without proper training, SI employees and other affiliated persons may not know to report information spillage in a timely manner, which would hinder the Privacy Council's effectiveness in mitigating breaches in a timely manner. Although somewhat mitigated by the additional *Privacy 101* training, it is possible that individuals outside of the targeted groups may handle PII or sPII.

System-level

(4) Five of seven sampled systems had not yet completed a Privacy Threshold Analysis and Privacy Impact Analysis despite the fact that some of these systems process confidential

and sensitive personnel data such as employees' medical records and biometric facial and fingerprint information.

According to Smithsonian Directive (SD) 118, *Privacy Policy,* a PTA and Privacy Impact Analysis should be completed for all IT systems that are designed to collect PII and/or sPII. A PTA is required for all technology or digital projects (e.g., websites, IT systems, or mobile applications) that collect, use, store, or disseminate PII or sPII. The SPO uses the PTA information to identify potential privacy issues, ensure compliance with applicable privacy policies and laws, and determine if additional privacy documentation is necessary. A SPIA is an additional questionnaire completed as part of the Privacy Review and Approval Process as a second step after a PTA.

Williams Adley requested the completed PTA and Privacy Impact Analysis for the seven systems selected for testing. OCIO and the Privacy Office were unable to provide a completed PTA or Privacy Impact Analysis for five of the seven systems. Four systems—IDMS, SMS, ePMX, PSCMS—were still in the process of developing the PTA and Privacy Impact Analysis. The system owner for the fifth system, Tessitura, was not aware that a PTA and Privacy Impact Analysis was required. The Tessitura system owner stated that it was his understanding that a PTA and Privacy Impact Analysis were needed only for new systems and for existing systems implementing a material change that would result in the new collection, use, storage, or dissemination of PII and sPII. The policy, however, states that all systems that use, store, or disseminate PII or sPII must have a PTA and a Privacy Impact Analysis, not only new systems. Without completion of the PTA and Privacy Impact Analysis, systems may operate without SPO's knowledge of PII and sPII data usage. Adequate privacy controls may not be built into the system and the risk to the data and to SI's reputation may not be assessed.

Security Training

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

For FY2018, the Security Training program operated at Level 3: Consistently Implemented. OCIO improved the security training domain by tracking completion metrics related to security awareness and training activities. OCIO also measured the effectiveness of its awareness training program by conducting phishing exercises and following up with additional training, and/or disciplinary action, as appropriate. SI also maintains specialized security training completion records via the automated GRC tool. However, Williams Adley noted that OCIO management had not formalized a needs assessment to guide training requirements and ensure efficient allocation of training resources.

Entity-level

(1) OCIO did not conduct the needs assessment within all the functional areas.

NIST 800-50[8] recommends that a high-level security training strategy have the following components: structure of the awareness and training program, priorities, funding, goals of the program, target audiences, types of courses and material for each audience, and use of technologies. NIST 800-50 further states, "completion of the needs assessment allows an agency to develop a strategy for developing, implementing, and maintaining its IT security awareness and training program." In July 2018, Williams Adley requested a copy of the FY2018 needs assessment and was informed by OCIO management that there was no formal needs assessment. OCIO management personnel stated that OCIO uses a broad and generalized approach to training rather than targeting through a needs assessment. OCIO management personnel do track security trends and update general security awareness training annually, with input from individuals throughout SI. Without a needs assessment, OCIO may be unable to effectively target its limited training resources on the most important security knowledge gaps.

III. Detect

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

In FY2018, the Detect function operated at Level 2: Defined. OCIO had not fully implemented its multi-year information security continuous monitoring strategy, which is a major component of the Detect function.

Information Security Continuous Monitoring

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[9] Without a fully implemented ISCM program, OCIO may not detect attempts to damage its systems, resulting in unauthorized access, data loss, operational failure, or unauthorized data modification. OCIO also would be unable to produce the key security metrics needed to measure and monitor the effectiveness of its current information security posture.[10]

In FY2018, ISCM operated at Level 2: Defined. OCIO improved its ISCM program by developing ISCM policies and procedures to support the ISCM strategy and completing a list of metrics for analyzing ISCM performance measures and reporting findings. Williams Adley, however, noted that OCIO did not have a process for monitoring all of the metrics.

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

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

[10] 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.

Entity-level

(1) OCIO had not yet completed the implementation of its ISCM strategy.

According to NIST 800-137,

> *An effective ISCM begins with development of a strategy that addresses ISCM requirements and activities at each organizational tier (organization, mission/business processes, and information systems). Each tier monitors security metrics and assesses security control effectiveness with established monitoring and assessment frequencies and status reports customized to support tier specific decision making.*

OCIO defined an ISCM strategy that meets ISCM requirements and includes specific activities, but was still working to implement the full strategy. OCIO broke the ISCM strategy into four phases, but with no defined completion dates for the phases or a target date for overall completion. The ISCM strategy implementation will continue into FY2019, with OCIO planning to further expand the information being collected, develop additional alerts, enhance monitoring, refine documentation of the monitoring, and develop automated data feeds between tools.

As of the end of FY2018, OCIO had completed Phases 1 and 2 and was working on Phase 3. For the portion of the plan that was already implemented, Williams Adley's review noted that OCIO had established a limited set of metrics and alerts. For example, OCIO is tracking attempted external attacks against the SI; however, OCIO management stated that they are still in the process of developing all identified metrics in the automated GRC tool for tracking and reporting. Per OCIO management, SI did not complete implementation of its ISCM strategy due to resource constraints. Until the ISCM strategy is fully implemented, including the monitoring of all critical metrics and risks, OCIO may have gaps in the security of some or all information systems.

IV. Respond

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

In FY2018, the Respond function operated at Level 2: Defined. OCIO made several improvements in the Incident Response program; however, Williams Adley determined that those improvements were not in place until June 2018.

Incident Response

Technical Note IT-930-TN30 states, *IT Security Incident Response Procedures*, "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 about where it is most cost effective to focus security resources.

For FY2018, SI's incident response program operated at Level 2: Defined. Improvements during FY2018 included OCIO updating its incident response policies to align with United States Computer Emergency Readiness Team (US-CERT) reporting requirements. One important

update included prioritizing incidents by US-CERT categorizations to better assess the impact of an incident on the environment. In addition, OCIO finalized implementation of the Security Information and Event Management (SIEM) tool in June 2018, but did not have a fully implemented incident response program until the same time period.

Entity-level

(1) OCIO did not have an up-to-date incident response program, aligned with US-CERT guidance, until June 2018.

OCIO's Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2*, IR-05 states, "the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information." On June 18, 2018, OCIO released an updated incident response policy that addressed missing elements identified in the FY2017 information security program review.[11] The updated procedures required the use of an incident response tracking and reporting tool.

Williams Adley reviewed SINet security incidents that occurred throughout FY2018, and found that OCIO had implemented tools to support some incident response activities; however, OCIO did not implement the key incident response tool until June 2018.

Before June 2018, Williams Adley's testing identified that OCIO did not report all security incidents to US-CERT[12] within the US-CERT–mandated timeframe. OCIO's Technical Note IT-930-TN30, *IT Security Incident Response Procedures*, required SI to report to US-CERT within the timeframes defined based on the category of the incident. Williams Adley determined that five of seven incidents were not reported in accordance with documented policies and procedures. Specifically, three of five incidents were not reported to US-CERT in a timely manner, and two of five incidents were not reported to US-CERT.

Williams Adley also determined that SI did not meet current US-CERT reporting requirements before implementing the current procedures in June 2018. Williams Adley reviewed OCIO's *IT Security Incident Response Procedures*[13] and noted that seven areas required by NIST were not documented. Specifically, the following NIST requirements were not formally documented in a policy, procedure, or plan before implementing the current plan in June 2018: (1) identification of major incidents; (2) incident response correlation[14]; (3) insider threat program[15]; (4) common threat vector taxonomy[16]; (5) metrics for measuring the incident response capability and

[11] Williams, Adley & Company-DC, LLP, *Fiscal Year 2017 Information Security Program Review*, September 18, 2014.

[12] US-CERT is the federal civilian government's focal point for computer security incident reporting, providing assistance with incident prevention and response 24 hours per day. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

[13] Technote IT-930-TN30, *IT Security Incident Response Procedures*, January 6, 2015.

[14] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[15] NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

[16] A Threat Vector is a path or a tool that a Threat Actor, such as a hacker, uses to attack the target. The taxonomy will classify the threat vectors.

effectiveness;[17] (6) roadmap for maturing the incident response capability[18]; and (7) how the program fits within the overall organization.[19]

During FY2018, OCIO stated that there was a change in the incident response leadership position, and that the incident response program transitioned after the new incident response leadership took effect. The new incident response manager prioritized changes to policies, procedures, and tool usage. Until the current guidance and supporting tools were released, major incidents may not have been prioritized, which could have increased the risk to information security.

System-level

(2) System owners for one of seven sampled systems did not define system-specific incident response procedures as required.

According to IT-930-TN30, *IT Security Incident Response Plan and Procedures*,

> *It is the responsibility of each system owner to ensure that specific incident management procedures are developed for their system and that those procedures adhere to and integrate with the procedures in this technical note. The system IR procedures must specify incident management roles and responsibilities for the system and must ensure that the system's users and administrators are trained on their responsibilities regarding incident reporting and response within the system.*

Williams Adley requested the TSA Tessitura incident response procedures and was informed by TSA Tessitura system owners that they do not have system-specific procedures. Instead, they followed OCIO guidelines and they did not have defined incident response roles and responsibilities at the system level. TSA Tessitura management were not aware that they needed to coordinate efforts and resources to develop system-specific procedures to support its incident response program. Without the supporting procedures, TSA Tessitura may not be able to detect, identify, contain, eradicate, and recover from security incidents. Also, if specific incident-response roles are not defined, TSA Tessitura staff may not be aware of their roles in the incident response process supporting OCIO.

(3) SI did not perform annual incident response testing for three of seven systems tested.

According to Technical Standards & Guidelines IT-930-02, *Security Control Manual*, control IR-03 states, "the organization tests the incident response capability for the information system at least annually using table top exercises or simulation exercises to determine the incident response effectiveness and document the results."

Williams Adley requested ePMX and Tessitura incident response testing and was informed by ePMX and Tessitura owners that they did not complete system-level incident response training and testing. ePMX and Tessitura system owners stated they did not know they needed separate system-level incident response processes as they fit within OCIO's. By not performing incident response testing, ePMX and Tessitura would not be able to evaluate the effectiveness of their

[17] NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012.

[18] NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012.

[19] NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012.

incident response or to leverage crucial information from the testing to enhance their incident response processes.

The *HRMS System Security Plan* states that the enterprise resource planning (ERP) incident response and disaster recovery personnel should test incident response and disaster recovery procedures annually, including an annual simulated event for disaster recovery and incident response. HRMS management informed Williams Adley that HRMS did not conduct incident response training and testing in FY2018. Management recognized this deficiency and established a plan to fix it by December 21, 2018. By not performing annual incident response testing, HRMS would not be able to evaluate the effectiveness of its incident response or to leverage crucial information from the testing to enhance its incident response processes.

V. Recover

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

In FY2018, the Recover function operated at Level 2: Defined. The Recover process progressed from maturity Level 1: Ad-hoc in FY2017 because OCIO updated policies and procedures to support its IT contingency planning program. However, by the end of FY2018, OCIO was still working to conduct a business impact assessment to guide its recovery practices, with a target completion date of August 30, 2019.

Contingency Planning

The primary purposes of contingency planning are to prepare for rare events that have the potential for significant consequences and to escalate events to address high-priority risks first. Without an effective entity-wide contingency planning program, IT systems may be unavailable to support mission and critical operations. Large-scale system problems, such as those stemming from a major security breach or a natural disaster, can result in competing priorities with respect to recovery efforts. If planning has not been sufficient, prioritization decisions must be made in real time without the benefit of deliberate analysis, which might result in errors, rework, and delayed recovery.

In FY2018, OCIO took steps to improve its contingency planning program. For example, OCIO consistently implemented its processes and technologies for information system backup and storage, including using alternative storage and processing sites, as appropriate. Alternative processing and storage sites are selected based on risk assessments that minimize the potential for disruption to the SI's ability to initiate and sustain operations, and that are not subject to the same physical and/or cybersecurity risks as the primary sites. OCIO also ensured that backups of information at the user and system levels were consistently performed and that the confidentiality, integrity, and availability of the information was maintained. Finally, OCIO implemented a different technology for infrastructure recovery by adopting Amazon Web Services (AWS). User systems are now backed up daily and data are pushed out to AWS and updated. However, OCIO was still working to address a FY2017 review recommendation to conduct a business impact analysis to guide the disaster recovery plan, with a target date of August 30, 2019.

System-level

(1) IDMS did not fully implement communication protocols associated with recovery activities.

The *OPS SMS/IDMS Disaster Recovery Plan*, updated August 2018, requires the Technical Recovery Team to hold regular meetings to improve communication among team members. Williams Adley requested supporting evidence of the disaster recovery meetings in FY2018, but OPS did not provide evidence that the required Technical Recovery Team meetings were held in FY2018. OPS officials stated that OPS personnel staff changes and updates were reflected in the Disaster Recovery Plan on August 22, 2018; however, no Technical Recovery Team meetings occurred either before or after the personnel staff changes in FY2018. Without developed and practiced communication procedures for recovery activities, miscommunication during an incident could lead to errors and rework, further delaying recovery.

Conclusion

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

Recommendations

Identify

Recommendation 1: The OPS system owner review and update its signed agreements with all contractor systems, in accordance with IT-930-02, Security Controls Manual Version 4.2.

Protect

Recommendation 2: The Chief Information Officer assess the highest risk privileged accounts within the environment and implement a multi-factor solution to harden against unauthorized use.

Recommendation 3: IDMS, Tessitura, ePMX, HRMS, and PSCMS owners ensure that system policies and procedures are in accordance with the Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.2.*

Recommendation 4: The Chief Information Officer develop and implement a process that ensures high vulnerabilities are remediated in accordance with the timeframes specified in Technote IT-930-TN33, *Vulnerability Management Program*.

Recommendation 5: TSA Tessitura system owners conduct periodic reviews of user accounts, in accordance with Technote IT-930-TN37, *Securing IT Accounts*.

Recommendation 6: The Chief Information Officer update security awareness training to include Information Spillage response, personally identifiable information handling procedures, and data collection requirements.

Recommendation 7: The Chief Information Officer assess current network operations and determine the best tool to prevent the intentional or unintentional exfiltration of PII.

Respond

Recommendation 8: The HRMS, and TSA Tessitura system owners develop and implement incident response procedures, including incident response training and testing, in accordance with IT-930-TN30, *IT Security Incident Response Plan and Procedures*.

Recover

Recommendation 9: OPS ensure that Technical Recovery Team meetings occur on the required basis and that these meetings are documented.

Smithsonian Institution

Office of the Chief Information Officer

Date: September 9, 2019

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

CC: Mike McCarthy, Acting Undersecretary for Finance and Administration
Greg Bettwy, Chief of Staff
Judith Leonard, General Counsel
Porter Wilkinson, Chief of Staff to the Regents
Joan Mockeridge, Office of Inspector General
Chuck Mitchell, Office of Inspector General
Juliette Sheppard, Director of IT Security
Danee Gaines Adams, Privacy Officer
Carmen Iannacone, Chief Technology Officer
Michael Delano, Smithsonian Enterprises, Director - Business Technology Operations
Kevin Holmes, Supervisory IT Specialist
Douglas Hall, Deputy Director, Physical Security and Business Operations
Curtis Lutz, Director HR & Admin Systems Division
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: Management Response to "*Fiscal Year 2018 Evaluation of the Smithsonian Institution's Information Security Program.*"

Thank you for the opportunity to comment on the report. We appreciate OIG's engagement in discussing the findings and revising the report based on discussion of the draft.

The Institution continues to make enhancements to the IT Security Program. Some key improvements in FY 2018 included:

- Migrated to new next generation firewalls
- Implemented automated Archer Security Incident Management tool and revised incident response process
- Successfully completed PCI DSS Level 2 merchant compliance assessment and submission
- Implemented automated Archer Privacy Assessment tool
- Migrated to new web vulnerability scanning tool
- Implemented SPF, DMARC, DKIM for email security
- Completed an enterprise System Inventory
- Initiated penetration testing for the PCI environments
- Authorization, Patching, Account Management, and Plan of Actions and Milestones processes.

- Implemented additional Splunk monitoring alerts, dashboards, and procedures.
- Updated IT Security Program Plan, ISCM Strategy, Enterprise Risk Assessment, and various policy and procedure documents
- Made improvements to Vulnerability Management, System Assessment and
- Implemented new improved Disaster Recovery infrastructure and program using AWS
- Migrated to Office365 and implemented security features such as email Data Loss Prevention

Regarding the audit report recommendations, Management provides the following responses.

Recommendation 1: The OPS system owner review and update its signed contracts with all contractor systems, in accordance with IT-930-02, Security Controls Manual Version 4.2.

Management concurs with this recommendation. However, the issue is not with a contract, but with an agreement with the Office of Personnel Management (OPM). Effective October 1, 2019, the National Background Investigation Bureau (NBIB) will transfer from the Office of Personnel Management (OPM) to the Department of Defense (DoD), and will be renamed the Defense Counterintelligence and Security Agency (DCSA), which was formerly known as the Defense Security Service (DSS). Our NBIB Agency Liaison recommended that we wait for the transition to DCSA to be completed and then a new MOU be obtained. OPS/PSIO will continue to use OPM's system until approximately the summer of 2020, and will then transition to using DCSA's systems which will require a MOU with DoD/DCSA. As such, OPS/PSIO concurs with the NBIB Agency Liaison and will wait to establish a MOU with DCSA/DoD. DCSA will provide the MOU templates to all agencies during the last quarter of CY 2019 or first quarter of CY 2020. Management expects the new MOU to be completed by July 2020.

Recommendation 2: The Chief Information Officer assess the highest risk privileged accounts within the environment and implement a multi-factor solution to harden against unauthorized use.

Management concurs with this recommendation and has already implemented the necessary remediations. OCIO has segmented the most sensitive Active Directory administration accounts (Tier 0) from lower-tier accounts. These accounts were further hardened by adding them to a "Protected Users" security group, placing restrictions on their access, and requiring multi-factor authentication. OCIO staff verified the new controls, leveraging the same tools and techniques used in the external audits, and found them to be effective at significantly reducing the risk of compromise. Management considers this recommendation completed.

Recommendation 3: IDMS, Tessitura, ePMX, HRMS, and PSCMS owners ensure that system policies and procedures are in accordance with the Information Technology Technical Standards & Guidelines IT-930-02, Security Controls Manual Version 4.2.

Management concurs with this recommendation. The listed systems have all now completed documentation of the cited key process areas (e.g., account management, change management, incident response, etc.). IDMS (which includes PSCMS as a sub-component) and HRMS have also now completed full re-ATO through the revised Assessment and Authorization process. As a

side note, upon further analysis, ePMX has been re-classified as a minor system. Management considers this recommendation completed.

Recommendation 4: The Chief Information Officer develop and implement a process that ensures high vulnerabilities are remediated in accordance with the timeframes specified in Technote IT-930-TN33, Vulnerability Management Program.

Management concurs with this recommendation and has already implemented the necessary remediations. A new process has been developed and implemented to escalate vulnerabilities that are not remediated within the required timeframes or which require expedited resolution. The process escalates the vulnerabilities to management attention and can result in blocking of un-remediated systems and devices from the Smithsonian network. OCIO also implemented automated vulnerability reports and dashboards to improve communication of vulnerability information to customers and conducted several training sessions on use of the scanning reports. System owners have been granted access to the scanning tools for their hosts and web applications so that they can review, assess, and remediate vulnerabilities in a timely manner. Additionally, enhancements have been made to the Software Review Board (SRB) process to highlight the most vulnerable hosts, in addition to software, for prioritized remediation. Management considers this recommendation completed.

Recommendation 5: TSA Tessitura system owners conduct periodic reviews of user accounts, in accordance with Technote IT-930-TN37, Securing IT Accounts

Management concurs with this recommendation. TSA had been performing regular audits of Tessitura user accounts but had not been documenting their completion. These audits, including the process and the audit results, are now documented. Management considers this recommendation completed.

Recommendation 6: The Chief Information Officer update security awareness training to include Information Spillage response, personally identifiable information handling procedures, and data collection requirements.

Management concurs with this recommendation. Content regarding Information Spillage has already been incorporated into the security awareness training as of FY 2019. Since the FY2020 course has already been finalized with the training vendor, OCIO will address the other Privacy topics in the Fiscal Year 2021 security awareness training. This training will be implemented by December 31, 2020.

Recommendation 7: The Chief Information Officer assess current network operations and determine the best tool to prevent the intentional or unintentional exfiltration of PII.

Management concurs with this recommendation. OCIO already has a project on the architecture roadmap related to network Data Loss Prevention (DLP). However, this project is dependent on funding requested in the FY21 federal budget submission. OCIO will assess and determine the most appropriate DLP tool to prevent inappropriate PII exfiltration and document a plan by

March 31, 2021.

Recommendation 8: The HRMS, and TSA Tessitura system owners develop and implement incident response procedures, including incident response training and testing, in accordance with IT-930-TN30, IT Security Incident Response Plan and Procedures.

Management concurs with this recommendation and has already implemented the necessary remediations. Since the time of the audit, both HRMS and TSA Tessitura have documented the necessary procedures and held incident response training and tabletop testing exercises. However, it should be noted that with enhanced centralization of incident response processes, the requirements in IT-930-TN30 are currently being updated to require systems to comply with central incident response processes managed by the Security Operations Center and only document the list of personnel with system-level incident responsibilities. Management considers this recommendation completed.

Recommendation 9: OPS ensure that Technical Recovery Team meetings occur on the required basis and that these meetings are documented.

Management concurs with this recommendation. OPS will develop a schedule of meetings, including disaster recovery and tabletop exercises. The meetings that are held will be documented. This will be completed by March 1, 2020.

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

Appendix A – Guidance

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

Office of Management and Budget (OMB) Memorandum (M)-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, November 4, 2016.

I. Risk Management

a. NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and System View,* March 2011
b. NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010
c. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013
d. NIST SP 800-60 Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
e. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Security Systems,* February 2004
f. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011
g. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, July 2017
h. SI Technote IT-930-03, *Security Assessment & Authorization,* January 2017
i. SI Technote IT-930-TN34, *IT Security System Inventory,* August 2015
j. SI Technote IT-930-TN29, *IT Security Plans of Action and Milestones,* June 2015
k. SI Technote IT-930-TN22, *Security Agreements for Interconnected Systems,* October 2006
l. SI Technote IT-960-TN31 *Security Configuration Management of Baselines,* September 2012

II. Configuration Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, July 2017
b. *Smithsonian Astrophysical Observatory Scientific Computing Infrastructure Configuration Management Plan Version 2.1*, September 2015

III. Identity and Access Management

a. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, July 2017
b. SI Technote IT-930-TN37, *Securing IT Accounts,* October 2015

IV. Security Training

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

V. Information Security Continuous Monitoring

a. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011
b. *Smithsonian Institution Information Security Continuous Monitoring*, December 2016
c. SI Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, July 2017
d. SI Technote IT-930-TN33, *Vulnerability Management Program,* July 2015

VI. Incident Response

a. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013
b. NIST 800-61 Revision 2, *Computer Security Incident Handling Guide,* August 2012
c. *FY 2017 CIO* [Chief Information Officer] *FISMA Metrics* Version 1, October 2016
d. Department of Homeland Security (DHS) EINSTEIN (https://www.dhs.gov/einstein), June 2017
e. SI Technote IT-930-TN30, *IT Security Incident Response Procedures,* January 2015
f. *US-CERT Federal Incident Notification Guidelines*

VII. Contingency Planning

a. NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010
b. SI Technote IT-960-TN46, *Backup and Data Recovery*, April 2017
c. Technical Standards & Guidelines IT-960-02, *Disaster Recovery Planning*, January 2003
d. *Office of Protection Services Security Management System / Identity Management System Disaster Recovery Plan*, August 22, 2018
e. *Office of System Modernization Disaster Recovery Plan*, September 28, 2018
f. *Infrastructure Disaster Recovery Plan "High Level Common Components,"* January 2018

Appendix B – Smithsonian OIG's Fiscal Year 2018 Submission to CyberScope

Overall	
FISMA Question	**FY2018 Assessment**
0.1 - Please provide an overall IG self-assessment rating (Effective/Not Effective).	Overall Level 2: Defined – Not Effective
0.2 - Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.	Williams Adley selected two moderate-impact Smithsonian Institution systems—SINet and Identity Management System (IDMS)—to perform detailed testing for the FY2018 FISMA audit. Williams Adley selected five moderate-impact Smithsonian Institution systems—Personnel Security Case Management System (PSCMS), Security Management System (SMS), Human Resource Management System (HRMS), ePMX, and Tessitura—to perform additional testing for the Protect and Respond functions of the FY2018 FISMA audit. Based on our discussions with Smithsonian Institution personnel and our inspection of the supporting documentation, the Smithsonian Institution has developed strategies and plans for most FISMA domains. The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on the assessment of Smithsonian Institution's information security program, the overall maturity level is Level 2: Defined.

Function: Identify – Risk Management	
FISMA Question	**FY2018 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: CA-3, PM-5, and CM8; OMB	**Level 2: Defined** – Smithsonian Institution has defined procedures to complete the authorization to operate (ATO) package for all information systems. However, Smithsonian Institution is in the process of identifying a comprehensive and accurate inventory of its information systems. The inventory

M-04-25; NIST 800- 161; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4; FY 2018 CIO FISMA Metrics: 1.1 and 1.4)?	is expected to be completed in FY2019. In addition, IDMS' ATO package is in the process of getting re-authorized and is expected to be completed in FY2019.
2 - To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2; FY 2018 CIO FISMA Metrics: 1.2)?	**Level 2: Defined** – Smithsonian Institution has defined a process for using standard data elements/taxonomy to develop an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting. However, Smithsonian Institution did not have an up-to-date hardware inventory because most of its information systems were in the process of being re-authorized by the end of FY2018.
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: CA-7, CM8, and CM-10; NIST SP 800137; FEA Framework, v2)?	**Level 2: Defined** – Smithsonian Institution has defined a process for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets connected to the organization's network with the detailed information necessary for tracking and reporting. However, Smithsonian Institution did not have an up-to-date software inventory or software license inventory list because most of its information systems were in the process of being re-authorized by the end of FY2018.
4 - To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that 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: 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)?	**Level 2: Defined** – Smithsonian Institution has categorized and communicated the importance and priority of information systems in enabling its missions and business functions. Smithsonian Institution rated IT security as one of the top 25 risks to the agency. However, because not all the systems are re-authorized, Smithsonian Institution is still in the process of categorizing all information systems.

5 - To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that 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: 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)?	**Level 2: Defined** – Smithsonian Institution has defined an information security risk management strategy and supporting policies and procedures. However, the entity-wide risk management strategy was not finalized.
6 - To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk, including risk from the organization's supply chain (NIST SP 800-39; FEA Framework; NIST SP 800-53: PL-8, SA-3, SA-8, SA-9, SA12, and PM-9; NIST SP 800161; DHS Binding Operational Directive 17-01)?	**Level 1: Ad-hoc** – Smithsonian Institution has defined and begun implementing the information security continuous monitoring strategy. However, Smithsonian Institution did not fully define the information security architecture.
7 - To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2; OMB A-123; CFO Council ERM Playbook)?	**Level 2: Defined** – Smithsonian Institution has defined the roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer/Senior Accountable Official for Risk Management, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission-specific resources. However, Smithsonian Institution has not finalized an entity-wide risk management strategy.
8 - To what extent has the organization ensured that plans of action and milestones (POA&Ms) are	**Level 2: Defined** – Smithsonian Institution has defined policies and procedures for POA&M maintenance, tracking, review, and validation to ensure the POA&Ms have all of the information needed to be closed. However, because the

utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?	Smithsonian Institution had not completed re-authorizing all systems, not all POA&Ms were being properly maintained.
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 800-37; NIST SP 800-39; NIST SP 800-53: PL-2 and RA-1; NIST SP 800-30; CSF:ID.RA-1 – 6)?	**Level 2: Defined** – Smithsonian Institution has a defined Information Security Risk Assessment procedure that includes threats, vulnerabilities, and impacts. However, not all risk assessments were completed by the end of FY2018.
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))?	**Level 2: Defined** – Smithsonian Institution has defined how information security risks are communicated in a timely manner to all necessary internal and external stakeholders. However, the risk management committee meetings at the entity-level, are conducted on an ad-hoc basis. Currently, SI is exploring training, deep-dive workshops, and online training as a means to ensure individuals understand how to identify and communicate risk at the entity level. Finally, because all information systems have not completed the ATO process, not all risks may be identified and communicated.
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 (FAR Case 2007-004; Common Security Configurations; FAR	**Level 2: Defined** – Smithsonian Institution has defined policies and procedures that require specific security FAR clauses, clauses on the protection of PII and reporting of information, as well as a requirement for a memorandum of understanding and an interconnection security agreement to be completed. However, not all the signed contracts reviewed included the required clauses.

Sections: 24.104, 39.101, 39.105, 39.106, and 52.239-1; President's Management Council; NIST SP 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2018 CIO FISMA Metrics: 1.5; Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)?	
12 - To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?	**Level 2: Defined** – Smithsonian Institution has obtained and begun to implement a Governance, Risk and Compliance (GRC) tool, Archer, to provide a centralized view of risks across the entity's information systems. However, the Archer tool and the associated metrics and usage were not fully implemented at the end of FY2018. Also, not all information systems have been completed the ATO process and not all the required details are included in Archer.
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?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall incident response program is at Level 2: Defined.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Configuration Management	
FISMA Question	**FY2018 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: CM-1; SP 800-128: Section 2.4)?	**Level 2: Defined** – Smithsonian Institution has defined roles and responsibilities for configuration management stakeholders. However, not all information systems have developed a configuration management plan and identified stakeholders and their associated responsibilities, as required.

15 - To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?	**Level 2: Defined** – Smithsonian Institution has defined configuration management policies and procedures, but not all systems have defined procedures as required.
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: CM-1; NIST 800-128: 2.2.1)	**Level 2: Defined** – Smithsonian Institution has defined and dispersed comprehensive policies and procedures for managing the configurations of its information systems. Policies and procedures have been tailored to the organization's environment and include specific requirements. However not all systems have defined procedures as required.
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: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?	**Level 2: Defined** – Smithsonian Institution has defined and dispersed its baseline configuration and component inventory procedures. However, the Smithsonian Institution does not currently have a complete inventory of hardware and software.
18 - To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017	**Level 2: Defined** – Smithsonian Institution has defined baseline configurations at the system level. However, without a complete understanding of the hardware and software inventory, it is not possible to ensure common secure configurations have been implemented across the entirety of the Smithsonian Institution network.

CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?	
19 - To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?	**Level 2: Defined** – Smithsonian Institution has defined remediation processes, including patch management, to manage software vulnerabilities. However, 295 vulnerabilities identified in November 2017 were again identified in August 2018.
20 - To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?	**Level 2: Defined** – Smithsonian Institution has chosen not to implement a TIC because it is not applicable to its environment. However, Smithsonian Institution has taken measures to protect its network by blocking external connections and by implementing the Uniform Resource Locator (URL) filtering policy for external connections.
21 - To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the Change Control Board (CCB), as appropriate (NIST 800-53: CM--2, CM-3)?	**Level 2: Defined** – Smithsonian Institution has defined change control policies and procedures. However, not all system-level changes have defined policies and procedures regarding the CCB.
22 - Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our

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?	testing, Williams Adley determined that Smithsonian Institution's overall configuration management program is at the Ad-hoc level.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Identity & Access Management	
FISMA Question	**FY2018 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 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?	**Level 2: Defined** – Smithsonian Institution has defined roles and responsibilities for identity and access management. Smithsonian Institution is not an executive branch agency; therefore, Smithsonian Institution has not adopted FICAM.
24 - To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?	**Level 2: Defined** – Smithsonian Institution has a defined identity and access management strategy. However, it has neither developed a roadmap to implement strong authentication for all users nor implemented the Department of Homeland Security's Continuous Diagnostics Mitigation (CDM) program.
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 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?	**Level 2: Defined** – Smithsonian Institution has defined identity and access management policies and procedures. However, it does not have policies and procedures implemented for remote access and is not currently capturing lessons learned to improve the effectiveness of its ICAM policies and procedures.
26 - To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to	**Level 3: Consistently Implemented** – Smithsonian Institution has defined procedures for screening and assigning personnel risk designations. However,

granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?	not automated tool has been implemented that shares assigned risk designations across the organization with those who need to know.
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: AC-8, PL-4, and PS-6)?	**Level 2: Defined** – Smithsonian Institution has defined its processes for developing, documenting, and maintaining access agreements for individuals who access the Smithsonian network. However, not all access agreements were required or maintained at the system level.
28 - To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?	**Level 2: Defined** – Smithsonian Institution has implemented a strong authentication—Entrust security token—for all users for remote access. However, Smithsonian Institution decided not to implement use of strong authentication mechanisms for non-privileged users to access its facilities, networks, and systems because it is not an executive branch agency and is not required to have strong authentication for all users in the environment.
29 - To what extent has the organization implemented strong authentication mechanisms (PIV or 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: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?	**Level 2: Defined** – Smithsonian Institution has implemented strong authentication—Entrust security token—for all users for remote access. Smithsonian Institution has planned for the use of strong authentication mechanisms for privileged users to access its facilities, systems, and networks.
30 - To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged	**Level 2: Defined** – Smithsonian Institution has defined a process for provisioning, managing, and reviewing privileged-user accounts. However, ePMX and Tessitura neither log nor periodically review privileged-user account activities.

user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?	
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: AC--17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)? (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?	**Level 2: Defined** – Smithsonian Institution has defined its configuration requirements for remote access connections. However, there is no process for documenting or reviewing audit logs (e.g., list of defined auditable events) of activities by remote users using VPN or Citrix.
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?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall identity and access management program is at the Defined level.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Data Protection and Privacy	
FISMA Question	**FY2018 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; OMB M-18-02; OMB A-130, Appendix I; NIST SP 800-53: AR-4 and Appendix J)?	**Level 2: Defined** – Smithsonian Institution has defined a privacy program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems. However, not all privacy policies and procedures were up-to-date throughout FY2018: Smithsonian Directive (SD) 118, Privacy Policy has not been updated since March 11, 2014, and SD 119, Privacy Breach Policy, was finalized and posted on Prism (the Smithsonian's intranet site) on September 12, 2018.
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; Appendix J, SC-8, SC-28, MP-3, and MP-6; FY 2018 CIO FISMA Metrics: 2.9 and 2.10)? • *Encryption of data at rest* • *Encryption of data in transit* • *Limitation of transfer to removable media* *Sanitization of digital media prior to disposal or reuse*	**Level 2: Defined** – Smithsonian Institution has defined security controls to protect its PII and other sensitive data, as appropriate, throughout the data lifecycle, including using encryption of data at rest and data in transit, and limits on transfer to removable media. However, continuous monitoring of security controls across all information systems has not been fully implemented.
35 - To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53: SI3, SI-7(8), SI-4(4) and (18), SC7(10), and SC-18; FY 2018 CIO FISMA Metrics: 3.8 – 3.12)?	**Level 2: Defined** – Smithsonian Institution has defined security controls to prevent data exfiltration and enhance network defenses. However, data loss prevention tools still must be properly configured for effectiveness.
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: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M17-25)?	**Level 2: Defined** – Smithsonian Institution has defined a Data Breach Response Plan. However, not all privacy policies and procedures were up-to-date by the end of FY2018: SD 118, Privacy Policy, has not been updated since March 11, 2014, and SD 119, Privacy Breach Policy, was finalized and posted on Prism (the Smithsonian's intranet site) on September 12, 2018.
37 - To what degree does the organization ensure that privacy awareness training is provided to all	**Level 2: Defined** – Smithsonian Institution has defined privacy awareness training and role-based privacy training as mandatory for staff and affiliated

individuals, including role-based privacy training (NIST SP 800-53: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)	persons who handle PII as a regular part of their job responsibilities. However, privacy training is voluntary for the majority of SI staff. There is some high-level PII training provided within general security training, but it does not cover the required components, such as data collection requirements or the consequences for failing to carry out responsibilities.
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?	**Level 2: Defined** – The Department of Homeland Security considers Level 4: Managed and Measurable, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall data protection and privacy program is at Level 2: Defined. Smithsonian Institution must finish updating SD 118, Privacy Policy, which was last updated March 22, 2014; implement privacy training for all staff across the organization; and ensure that Privacy Assessments are completed for all information systems.
Calculated Maturity Level	**Level 2: Defined**

Function: Protect – Security Training	
FISMA Question	**FY2018 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 3: Consistently Implemented** – Smithsonian Institution has defined and communicated roles and responsibilities for the stakeholders involved in the security awareness and training program. In addition, stakeholders must have adequate resources (i.e., people, processes, and technology) to consistently implement security awareness and training responsibilities. Smithsonian's CSAT training is established agency-wide as well as role-based training.

40 - To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53: 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 1: Ad-hoc** – Smithsonian Institution did not conduct a skill gap assessment within all functional areas.
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: AT-1; NIST SP 800-50: Section 3).	**Level 2: Defined** – Smithsonian Institution has focused on tailoring its annual security awareness training and conducts internal reviews of all trainings annually to determine their appropriateness. However, there is no formalized GAP analysis to measure training requirements against the strategy.
42 - To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53: AT-1 through AT-4; and NIST SP 800-50).	**Level 4: Managed and Measurable** – Smithsonian Institution has defined security awareness and specialized security training policies and procedures. Smithsonian Institution also monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training policies and procedures. Smithsonian Institution ensures that data that support the metrics are obtained accurately, consistently, and in a reproducible format. Smithsonian Institution is able to provide evidence of tracking metrics related to security awareness and training activities.

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: AT2; FY 2018 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; SANS Top 20: 17.4).	**Level 4: Managed and Measurable** – Smithsonian Institution tailors security awareness training specifically to match the requirements identified as critical by the OCIO. OCIO measures the effectiveness of its awareness training program by conducting phishing exercises and following up with additional awareness or training and/or by carrying out disciplinary actions, as appropriate. Phishing exercises include sending users phishing emails multiple times.
44 - To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 80053: AT-3 and AT-4; FY 2018 CIO FISMA Metrics: 2.15)?	**Level 3: Consistently Implemented** – Smithsonian Institution ensures that individuals with significant security responsibilities are provided with specialized security training before they are given access to information systems, before they perform their assigned duties, and periodically thereafter, and maintains appropriate records (S-111). Also, personnel who have significant security responsibilities are required to complete continuing education hours based on their job descriptions annually. Smithsonian Institution maintains specialized security training completion records through Archer; however, there is no process in place to update or gather feedback on training for specialized security training.
45 - Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall security training program is at Level 3: *Consistently Implemented*. However, because Smithsonian Institution does not have a strategy to guide updates to an ever-changing security landscape and a current understanding of skills and associated gaps in security knowledge, Smithsonian Institution should not be considered to be at Level 4: Managed and Measurable, across the domain.

	Without these two steps, there could be security training that is not being completed or updated as needed.
Calculated Maturity Level	**Level 3: Consistently Implemented**

Function: Detect – Information Security Continuous Monitoring	
FISMA Question	**FY2018 Assessment**
46 - To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?	**Level 2: Defined** – Smithsonian Institution has defined an information security continuous monitoring (ISCM) strategy that meets ISCM requirements and activities. However, Smithsonian Institution did not consistently implement the ISCM strategy at the organization and system levels. The ISCM implementation plan will continue into FY2019.
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: CA-7) (Note: The overall maturity level should take into consideration the maturity of question 49)?	**Level 2: Defined** – Smithsonian Institution has defined ISCM policies and procedures to support the ISCM strategy. However, Smithsonian Institution did not consistently capture lessons learned to make improvements to its 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: CA-1; NIST SP 800-137; and FY 2018 CIO FISMA Metrics)?	**Level 2: Defined** – Smithsonian Institution has defined ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies. However, the ISCM process had not been fully implemented for personnel with ISCM responsibilities to carry out their duties at the system level.
49 - How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls	**Level 2: Defined** – Smithsonian Institution has defined a process for performing ongoing assessments, granting system authorizations, and monitoring security

(NIST SP 800137: Section 2.2; NIST SP 80053: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?	controls. However, the IDMS' ATO has not been completed in FY2018, and re-authorization has not started.
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** – **S**mithsonian Institution has completed a list of metrics for tracking purposes. Although there is not a process for monitoring all metrics, some ISCM metrics have been identified and some are now monitored as dashboards in Archer, but not all identified metrics have been set up in FY2018.
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?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall ISCM program is at Level 2: Defined.
Calculated Maturity Level	**Level 2: Defined**

Function: Respond – Incident Response	
FISMA Question	**FY2018 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: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800-184; OMB M-17-25; OMB M-17-09; FY 2018 CIO FISMA Metrics: 4.1, 4.3, 4.6, and 5.3; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 58).	**Level 2: Defined** – Smithsonian Institution has defined and communicated incident response policies, procedures, plans, and strategies. However, Smithsonian Institution did not consistently implement its incident response policies and procedures before implementing the current one in June 2018.
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	**Level 2: Defined** – Smithsonian Institution has defined and communicated the structures of its incident response teams; the roles and responsibilities of incident response stakeholders; and the associated levels of authority and dependencies. However, SMS, PSCMS, ePMX, and Tessitura have not defined and communicated the structures of the incident response teams; the roles and

organization (NIST SP 800-53: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2018 CIO FISMA Metrics: Section 4; and US-CERT Federal Incident Notification Guidelines)?	responsibilities of incident response stakeholders; and the associated levels of authority and dependencies.
54 - How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; and US-CERT Incident Response Guidelines)	**Level 2: Defined** – Smithsonian Institution has defined a common threat vector taxonomy and has developed handling procedures for specific types of incidents. However, while there are policies and procedures in place for supporting technologies used to detect and analyze potential incidents, Smithsonian Institution did not consistently implement those policies and procedures to support intrusion detection software and monitoring tools, such as intrusion detection systems (IDS) and Splunk, before SINet's ATO completion in August 2018.
55 - How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2)?	**Level 2: Defined** – Smithsonian Institution has defined processes for an incident response plan that include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems. However, after Smithsonian attempted to mitigate an incident that occurred in FY2018, the security issue persisted and continued to affect some Smithsonian websites in September 2018.
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; DHS Cyber Incident Reporting Unified Message)?	**Level 2: Defined** – Smithsonian Institution has defined its requirements for personnel to report suspected security incidents to the entity's help desk and/or security operations center within the defined timeframes. Smithsonian Institution also has defined its processes for reporting security incidents to US-CERT; however, in FY2018, not all incidents were reported to US-CERT in a timely manner.
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,	**Level 2: Defined** – Smithsonian Institution is not required to have a contract with DHS for Einstein implementation and does not use the DHS Einstein program for intrusion detection and prevention capabilities for traffic entering and leaving the Smithsonian Institution networks. However, Smithsonian

including through contracts/agreements, as appropriate, for incident response support (FY 2018 CIO FISMA Metrics: 4.4; NIST SP 800-86; NIST SP 800-53: IR-4; OMB M-18-02; PPD-41).	Institution is in discussions with DHS regarding implementation of the Einstein 3 program.
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 2: Defined** – Smithsonian Institution has used many tools to support the incident response program. However, while tools are implemented to support some incident response activities, Smithsonian Institution did not consistently use its technologies as an incident response process for FY2018. The incident response tracking and reporting tool was not implemented until June 2018, the SIEM tool configuration was completed in June 2018, and, finally, the data loss prevention tool does not prevent data loss, but rather notifies SI of a breach after the policy has been violated. In addition, the tool was disabled for PII detection in FY2018 before enabling a new data loss prevention rule in FY2019.
59 - Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of an overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall incident response program is at Level 2: Defined.
Calculated Maturity Level	**Level 2: Defined**

Function: Recover – Contingency Planning	
FISMA Question	**FY2018 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: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?	**Level 2: Defined** – Smithsonian Institution has a defined Smithsonian Emergency Management Program; an Emergency Planning Risk Action Plan; and a DRP document developed in 2003, which Smithsonian Institution is currently updating, with its estimated draft completion date in FY2019. However, the current version of the DRP does not reflect current National Institute of Standards and Technology (NIST) guidelines.
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 800161; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5).	**Level 2: Defined** – Smithsonian Institution has defined ISCP policies and procedures, which meets the requirement that every information system must have a documented ISCP. However, Smithsonian Institution has a defined DRP document, developed in 2003, but the document does not reflect current National Institute of Standards and Technology (NIST) guidelines. In addition, SI is currently updating the DRP, with its estimated draft completion date in FY2019.
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: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17-09; FY 2018 CIO FISMA Metrics: 5.6)?	**Level 1: Ad-hoc** – Smithsonian Institution neither defined a process for conducting a business impact analysis nor conducted a business impact analysis to guide contingency planning efforts.
63 - To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 80053: CP-2; NIST SP 800-34; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?	**Level 2: Defined** – Smithsonian Institution defined ISCPs for the two in-scope systems. However, there is no process in place to show how these information system contingency plans are coordinated with an entity-wide disaster recovery plan, continuity of operations plan (COOP), or business continuity plan.
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: CP-3 and CP4; FY 2018 CIO FISMA Metrics: 5.1, 5.2, and 5.5)?	**Level 2: Defined** – Smithsonian Institution has a defined process for performing tests and exercises of its information system contingency planning. However, there is no defined COOP or a process to test ISCPs in conjunction with the incident response plan, business continuity plan, or entity-wide disaster recovery plan.
65 - To what extent does the organization perform information system backup and storage, including	**Level 3: Consistently implemented** – Smithsonian Institution has consistently implemented its processes and technologies for information system backup and

use of alternate storage and processing sites, as appropriate (NIST SP 800-53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2018 CIO FISMA Metrics: 5.4; and NARA guidance on information systems security records)?	storage, including the use of alternative storage and processing sites and RAID, as appropriate. Alternative processing and storage sites are chosen based on risk assessments that ensure potential disruption of the Smithsonian Institution's ability to initiate and sustain operations is minimized and not subject to the same physical and/or cybersecurity risks as the primary sites. Smithsonian Institution also ensures that backups of information at the user and system levels are consistently performed and that 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: CP-2 and IR-4)?	**Level 2: Defined** – Smithsonian Institution has defined an infrastructure ISCP plan that addresses roles and responsibilities as well as communication requirements and has an up-to-date phone tree. There also is a developed disaster recovery plan for critical systems housed in the data center, with roles and responsibilities and communication processes. However, for one of two in-scope systems, scheduled meetings to discuss disaster recovery were not apparent. Also, there were review comments in an additional in-scope system contingency plan that had not been resolved.
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 above and based on all testing performed, is the contingency program effective?	The Department of Homeland Security considers Level 4: *Managed and Measurable*, an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall incident response program is at Level 2: Defined.
Calculated Maturity Level	**Level 2: Defined**

Appendix C – System Descriptions

Williams Adley presents information on each of the seven in-scope systems that were evaluated as part of the FY2018 Information Security Program Review, as follows:

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

2. Identity Management System (IDMS) is sponsored by the SI Office of Protection Services (OPS). The IDMS is used for background investigations and identity proofing along with an automated electronic enrollment and biometric data management system. The system has links to OPM as well as online forms. The IDMS enables electronic capture and submission of biometric facial and fingerprint information for use in background checks and for tracking the status of background investigations. The IDMS is a business process that makes the credential issuance process more secure at SI. A standardized process for background investigations, credential issuance, and access control would streamline the process, improve security, and enable SI to address Homeland Security Presidential Directive 12 (HSPD-12) guidelines when appropriate.

3. Personnel Security Case Management System (PSCMS) handles critical personnel security functions, such as providing results for Office of Personnel Management (OPM) background investigations. The PSCMS component server is monitored by the Network Operations Center (NOC).

4. The OPS Security Management System (SMS) subsystems commonly manage electronic security within the physical structure of the Smithsonian Institution. SMS comprises the Software House (SWH) ID Badge Server, SWH C*Cure Central Server, SWH C*Cure 800/8000 Servers, PSCMS Server, and IDMS Server systems. SMS manages physical access control (i.e., SI credential management, automated access control information throughout different SI buildings and locations, revocation of badges, and automated access control) and manages electronic security such as physical intrusion detection, CCTV systems, digital video recorders and intercoms, and security within a building or campus, including access control.

5. The ePMX system provides SI IT with a centralized location for managing the IT procurement process. ePMX is a web-based application that enables Smithsonian Enterprises (SE) IT to efficiently manage purchases centrally by offering a built-in approval, tracking, and reporting mechanism. ePMX, which runs on Internet Information Server (IIS), is hosted at the Herndon Data Center (HDC) and is available on SINet-connected computers.

6. The Enterprise Resource Planning Human Resource Management System (ERP HRMS) stores and processes confidential, sensitive personal data on each employee. Managers throughout the Smithsonian Institution use the ERP HRMS for proactive decision-making to manage human capital and core activities, including recruitment, electronic transmittal of

personnel actions, benefits administration, training, employee and labor relations, recording and reporting of workplace incidents and injuries, management of relevant occupational health and safety data, competencies, career planning, succession planning, and performance appraisal processing. All SI units use the system to manage personnel actions and employee information and to document occupational incidents, injuries (CA-1), and illnesses (CA-2) for employees. The Office of Human Resources uses the ERP system to manage positions, comply with regulatory requirements, and recruit, hire, train, promote, reassign, and retire personnel. The Office of Safety, Health, and Environmental Management uses the Medgate Occupational Health and Safety system (part of the ERP HRMS) to manage health and safety data for SI. The ERP HRMS operates within the SI internal network as a browser-based application.

7. Tessitura is the system TSA uses for customer relationship management and event management (e.g., ticketing, fundraising, summer camps, continuous education). TSA self-manages all Tessitura servers except for the two web servers, which are managed by the Office of the Chief Information Officer (OCIO) Web Management team.

Appendix D – Inspector General FISMA Metrics

The FY2018 IG FISMA metrics consist of eight domains, grouped into five functional areas that correspond to the NIST cybersecurity framework, as follows:

1. *Identify*
   - Risk Management – The purpose of risk management is to create a sustainable and repeatable process for identifying, assessing, and responding to risk. To manage risk, entities must understand the likelihood that an event will occur and the resulting potential impact. Using this information, entities can determine the acceptable level of risk for the delivery of services and express this as their risk tolerance. Plans of action and milestones (POA&Ms), an integral part of risk management, are used to make risk-based decisions when assessing and addressing vulnerabilities by helping to prioritize the remediation requirements.
2. *Protect*
   - Configuration Management – The purpose of configuration management is to manage the effects of changes or differences in configurations on an information system or network. Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information helps security managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their responsibility, enabling the managers to direct changes as required. The goal of configuration management is to make assets harder to exploit through better configuration.
   - Identity and Access Management – The primary purpose of identity and access management is to establish a process that ensures users and devices are authenticated[20] before access is granted. This process ensures they (device or person) are who or what they identify themselves to be. The goal of identity and access management is to ensure users and devices have the proper authorization[21] to access information and information systems.
   - Data Protection and Privacy – The primary purpose of data protection and privacy is to establish a program that ensures the security of personally identifiable information (PII). Such a program should include encryption of data, data access restrictions, PII training for all users, and a breach process to use in case of any identified loss of PII. Data Protection and Privacy is a new domain for FY2018 FISMA examination.
   - Security Training – Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This training helps ensure that personnel at all levels of the entity understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Entities that continually train their workforce in organizational security policy

[20] The process of identifying an individual, usually based on a username and password.

[21] Authorization allows the user to access various resources based on the user's identity, which is authenticated with a username and password.

and role-based security responsibilities have a higher rate of success in protecting their information.

3. *Detect*
   - Information Security Continuous Monitoring (ISCM) – The purpose of ISCM is to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture and operational readiness.
4. *Respond*
   - Incident Response – A security incident is any activity that occurs that is a threat to the security of information resources. Incidents can be intentional events or accidental events that jeopardize the availability, integrity, or confidentiality of the entity's information and systems. A well-defined incident response capability helps the entity detect incidents rapidly, minimize loss and/or destruction, identify weaknesses, and restore IT operations quickly.
5. *Recover*
   - Contingency Planning – Contingency planning involves the actions required to plan for, respond to, and mitigate the effects of damaging events. The primary purpose of contingency planning is to prepare for rare events that have the potential for significant consequences and to promote first-priority risk.