Smithsonian Institution
Office of the Inspector General

In Brief

Fiscal Year 2017 Independent Evaluation of the Smithsonian Institution's Information Security Program

Report Number OIG-A-18-10, September 21, 2018

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 2017.

Background

The Department of Homeland Security and the Office of Management and Budget publish metrics each year 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 (level 1) state 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 the majority of the five cybersecurity functions, its information security program is considered effective overall.

What Was Found

For fiscal year 2017, Williams, Adley & Company - DC, LLP (Williams Adley) found that the Smithsonian Institution (Smithsonian) made improvements to its information security program. Significant improvements included updating the specialized security training program; adopting and beginning to implement a security information and event management tool; and adopting a governance, risk, and compliance tool to assist in security assessment and authorization.

However, the Smithsonian did not achieve the minimum maturity level defined by the Department of Homeland Security to be considered fully effective in fiscal year 2017. Williams Adley determined that the Smithsonian made progress in maturing its cybersecurity functions. For example, the Detect and Respond functions progressed from level 1: ad-hoc in fiscal year 2016 to level 2: defined in fiscal year 2017. While the Smithsonian has made considerable efforts to define policies and procedures for its program, additional work is needed to consistently implement them.

Williams Adley found that the maturity of the Smithsonian's information security program was hampered by an incomplete inventory of information systems, including related hardware and software components, and an information security architecture that was only partially defined. In addition, the Office of the Chief Information Officer had not yet defined an entity-wide disaster recovery plan based on a business impact analysis and had outdated guidance for configuration management and contingency planning. Further, Williams Adley found that, for the two information systems reviewed, there was minimal documentation in place to formalize their security practices.

What Was Recommended

Williams Adley made nine recommendations to enhance information security at the Smithsonian; management concurred with seven and partially concurred with two. For the partially concurred recommendations, management agreed with the key aspects of the recommendation and provided an explanation for an alternative implementation.

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

Smithsonian Institution
Office of the Inspector General

Memo

Date: September 21, 2018

To: David J. Skorton, Secretary

Cc: Albert Horvath, Chief Operating Officer and Under Secretary for Finance and Administration (OUSF&A)
Mike McCarthy, Deputy Under Secretary for Finance and Administration
Greg Bettwy, Chief of Staff, Office of the Secretary
Deron Burba, Chief Information Officer
Charles Alcock, Director, Smithsonian Astrophysical Observatory (SAO)
Juliette Sheppard, Director, Information Technology Security
Van McGlasson, Department Manager, Computation Facility, SAO

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

Subject: Fiscal Year 2017 Evaluation of the Smithsonian Institution's Information Security Program (OIG-A-18-10)

This memorandum transmits Williams, Adley & Company - DC, LLP's (Williams Adley) final report on the fiscal year 2017 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 2017, 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 seven of the nine recommendations, partially concurred with the other two recommendations, and proposed corrective actions.

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. Please call me or Joan Mockeridge, Assistant Inspector General for Audits, at (202) 633-7050, if you have any questions.

Smithsonian Institution Office of the Inspector General

Report on the Smithsonian Institution's Information Security Program

Fiscal Year 2017

September 21, 2018

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, 2017.

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 2017 FISMA audit report. Their response is presented in its entirety in Appendix C. 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, and 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 Kola A. Isiaq, Managing Partner, at (202)-371-1397.

Williams, Adley & Company-DC, LLP

September 21, 2018

Abbreviations

CCB	Change Control Board
CFO	Chief Financial Officer
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
CVE	Common Vulnerabilities and Exposures
CVSS V3	Common Vulnerabilities Scoring System Version 3
DHS	United States Department of Homeland Security
ERP	Enterprise Resource Planning
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Modernization Act
FMS	Facility Management System
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GRC	Governance, Risk and Compliance
HEA	High Energy Astrophysics
ICAM	Identity, Credential, and Access Management
SI	Smithsonian Institution
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OF&A	Office of Finance and Accounting
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SAO	Smithsonian Astrophysical Observatory
SCI	Scientific Computing Infrastructure
SD	Smithsonian Directive
SI	Smithsonian Institution
SIEM	Security Information and Event Management
SOC	Security Operations Center
SP	Special Publication
TIC	Trusted Internet Connection
TRB	Technical Review Board
US-CERT	United States Computer Emergency Readiness Team
VOIP	Voice Over Internet Protocol

Introduction

On behalf of the Office of the Inspector General (OIG), the auditing firm of Williams, Adley & Company-DC (Williams Adley) conducted an independent audit of the Smithsonian Institution's (SI) information security program and practices consistent with the Federal Information Security Modernization Act of 2014 (FISMA).

The FY 2017 FISMA CyberScope metrics consist of five cybersecurity framework security functions: Identify, Protect, Detect, Respond, and Recover. These five functions comprise seven FISMA domains: Risk Management, Configuration Management, Identity and Access Management, Security Training, Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning. The Department of Homeland Security (DHS) uses the FISMA CyberScope metrics to determine the maturity of an entity's information security program. The maturity levels range from Level 1: Ad-hoc to Level 5: Optimized. DHS defines an effective information security program as having reached a maturity of Level 4: Managed and Measurable.

Purpose

FISMA requires each executive branch entity to develop, document, and implement an entity-wide program to provide information security for the information systems that support the operations and assets of the entity. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of managerial, operational, and technical controls over information security.

FISMA requires the head of each entity to implement policies and procedures that cost effectively reduce information technology (IT) security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, 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.

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 the FY 2017 review, Williams Adley used the OIG FISMA CyberScope metrics to determine the status of SI's information security program. However, SI decided not to submit the FY 2017 CyberScope report to DHS.

Objectives, Scope, and Methodology

I. Objective

The objective was to conduct an independent audit of the effectiveness of SI's information security program and practices covering the period October 1, 2016, to September 30, 2017 (FY 2017).

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 two sampled SI systems, both with a security categorization of moderate: Smithsonian Astrophysical Observatory (SAO) Scientific Computing Infrastructure (SCI) and SAO High Energy Astrophysics (HEA).[1] Systems selected for testing are rotated annually among the approximately 48 major IT systems.

> *SAO SCI* is the general support system that supports the computing infrastructure and core services used by SAO employees to perform their daily work. The SAO SCI is composed of the networking and telecommunications IT infrastructure (routers, switches, virtual private network [VPN] and remote access servers, wireless access servers, domain name servers, intrusion detection systems, firewalls, and network monitoring systems), servers (scientific data reduction and compute servers, centralized authentication Network Information Systems [NIS], file and print, and Secure File Transfer Protocol [sFTP], data storage arrays, web servers and database engines, and PC and Windows desktops and scientific workstations. SAO SCI system users include the staff of the Harvard-Smithsonian Center for Astrophysics (both Harvard and SAO staff) and research collaborators throughout the world.
>
> *SAO HEA* is composed of the networking and telecommunications IT infrastructure (switches, remote access servers, network monitoring systems), servers (scientific data reduction and computing servers, centralized authentication NIS and Lightweight Directory Access Protocol [LDAP], file and print, email, Post Office Protocol [POP] and Internet Message Access Protocol [IMAP], email gateways, Simple Mail Transfer Protocol [SMTP] relays, and File Transfer Protocol [FTP]), data storage arrays, web servers, database engines, Unix and Linux desktops, PC and Windows desktops, and scientific workstations and servers. SAO HEA system users include the staff of the Harvard-Smithsonian Center for Astrophysics (both Harvard and SAO staff) and research collaborators throughout the world.

The SI OIG contracted Williams Adley to assess the effectiveness of SI’s information security program and practices. Williams Adley performed the audit from August 2017 through June 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 audit objectives.

To perform this audit, 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 judgmental sampling where applicable, inspected SI policies and procedures to supplement observations and

[1] The Smithsonian uses Federal Information Processing Standards Publication 199 to determine system security categorization.

interviews, and obtained sufficient evidence to support our conclusions and recommendations. Williams Adley also reviewed system-generated outputs (e.g., active directory lists) where possible to support our conclusions.

Background

I. The Smithsonian Institution

The SI was established by an Act of Congress signed by President James K. Polk on August 10, 1846. The SI is a trust instrumentality administered by a Board of Regents and a Secretary. Since its founding in 1846, 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 Financial Officer.

OCIO has primary responsibility for setting security policy, managing SI's security program, and evaluating IT system security for the approximately 48 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 Federal Information Processing Standards (FIPS) Publication 199.

III. 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 information system security.

Annually, OMB, in coordination with DHS, provides guidance on reporting categories and questions for meeting the current FY's reporting requirements.[4] OMB uses the data to assist in carrying out its oversight responsibilities and to prepare its annual report to Congress on entity compliance with FISMA. OMB and DHS gather the information from each organization using

[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 2016–2017 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-17-05, November 4, 2016.

three FISMA reports: (1) IG FISMA metrics, which can be found in Appendix B, (2) Senior Agency Official for Privacy (SAOP) FISMA metrics, and (3) Chief Information Officer (CIO) FISMA metrics. In FY 2017, the Smithsonian submitted IG metrics, but did not submit SAOP or CIO metrics to DHS.

The FY 2017 IG FISMA metrics consist of seven security processes, 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 impact. Using this information, entities can determine the acceptable level of risk for the delivery of services and express this as their risk tolerance. A plan of action and milestones (POA&M) is an integral part of risk management. POA&Ms 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, thus 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[5] before access is granted. This process ensures that 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[6] to access information and information systems.

   - 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

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

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

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 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 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.

Williams Adley used the IG metrics to assess each of the functions based on a maturity model. The model ranked the organization's maturity level on a scale of one to five using a series of 9–12 questions per level. Answers to each question were based on an assessment of both the entity-wide program and the two systems selected for testing. To move from Level 1 to Level 2, at least 50 percent of the Level 1 metrics must be met, 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 or above. The definition for each maturity level is shown in Figure 1.

Figure 1: Fiscal Year 2017 Maturity Model for FISMA Cybersecurity Functions

Level 5: Optimized
Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business and mission needs.

Level 4: Managed and Measurable
Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the entity and used to assess them and make necessary changes.

Level 3: Consistently Implemented
Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

Level 2: Defined
Policies, procedures, and strategy are formalized and documented, but not consistently implemented.

Level 1: Ad-hoc
Policies, procedures, and strategy are not formalized, and 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: FY 2017 IG FISMA Metrics

Results in Brief

For FY 2017, Williams Adley found that the Smithsonian Institution (SI) made improvements to its information security program, but did not have an effective program as defined by the Department of Homeland Security (DHS). This was because two of the five functions that Williams Adley were assessed at maturity Level 1: Ad-hoc, the lowest of the five maturity levels, and three of the five functions were assessed at maturity Level 2: Defined (see Appendix B for details). DHS requires that at least half of the five total cybersecurity functions be assessed at maturity Level 4: Managed and Measurable for the information security program to be considered overall effective.

At the program level, Williams Adley found that the maturity of SI's information security program was hampered by a system inventory that was not fully up to date and an information security architecture that was not yet fully defined. Williams Adley also found that SI's guidance for configuration management and contingency planning was outdated. In addition, the OCIO had not yet defined an entity-wide disaster recovery plan based on a business impact analysis. At the information system level, Williams Adley found that, for the two systems reviewed, there was minimal documentation in place to formalize their security practices.

Although the information security program did not reach an overall level of effective during FY 2017, Williams Adley determined that SI made progress in maturing each of the five cybersecurity functions. For example, the Detect, Respond, and two of the three subfunctions in Protect progressed to Level 2: Defined. Significant improvements included updating the specialized security training program; adopting and beginning to implement a security information and event management tool; and adopting a governance, risk, and compliance tool to assist in security assessment and authorization. While SI has made considerable efforts to define the program, additional work is needed to consistently implement policies and procedures. Until that work is complete, SI's sensitive data and assets will continue to be at risk.

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.[7] 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 FY 2017, the Identify function operated at Level 1: Ad-hoc, the lowest of five maturity levels. Although SI is making progress in maturing the Identify function, significant shortfalls remain that prevent SI from reaching the next maturity level, such as finalizing an information system inventory and establishing an information security architecture.

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 FY 2017, SI improved its risk management program by (1) implementing a risk management committee; (2) seeking experienced assistance about the risk management process; (3) implementing a comprehensive governance, risk, and compliance tool in OCIO; and (4) beginning a re-authorization process of all information systems. However, SI did not progress beyond Level 1: Ad-hoc due to the following five issues identified by Williams Adley's FY 2017 testing results.

[7] NIST, *Framework for Improving Critical Infrastructure Cybersecurity,* Feb. 2014.

Entity-level

(1) OCIO did not have a complete inventory in FY 2017 and did not require the collection of certain NIST-recommended data for information system components (hardware and software)

In FY 2017, OCIO had an incomplete inventory of information systems and related hardware and software components, but was in the process of updating this inventory in response to a prior audit recommendation. By the end of FY 2017, the inventory update was under way and was projected to be completed by December 2017. According to SI's OIG, OCIO completed the update to its inventory in January 2018.

In reviewing OCIO's guidance for maintaining an inventory of information systems and related components, Williams Adley found that OCIO's minimum required information for the components did not include data that Williams Adley believes are essential to assist in responding in a timely manner to information security incidents.

When using a centralized inventory, NIST 800-53 rev 4 control CM-8 states that effective accountability of information components requires the following data: hardware inventory specifications (e.g., manufacturer, device type, model, serial number, and physical location), software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses.

However, OCIO guidance required component name, type vendor, model, point of contact, and "other information necessary to achieve effective information system component accountability." Unlike the NIST guidance, OCIO did not define the "other information," leaving the individual systems' owners to determine what, if any, information to provide. As a result, OCIO has limited assurance that the information necessary for time-critical incident responses (e.g., software version numbers, network addresses, and physical location) will be readily available, and incident response could be delayed if such information is needed but not available.

(2) OCIO was still in the process of documenting an information security architecture that aligned with the SI strategic plan

At the end of FY 2017, OCIO was working to document an information security architecture, with a target date of December 31, 2018. Although the full architecture was not yet complete, OCIO documented and began implementing an ISCM strategy, which is part of the overall architecture. While an ISCM strategy helps to mitigate some security risk through monitoring, the information security architecture helps ensure that the security needs are aligned with business needs, security gaps are identified, and security capabilities, policies, and processes are aligned.

(3) OCIO did not have an automated tool in place to monitor IT security risks across the SI

NIST 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 FY 2017, SI began implementing an automated information security solution and tool to provide a centralized view of risks across SI's information systems. However, by the end of FY 2017, the tool and the associated metrics and usage were not fully implemented—less than 10 percent of major systems had been entered. Until the implementation is complete, SI will not be able to measure how well its information security program is managing the relevant IT security risks.

System-level

(4) SAO had expired agreements for operating the two sampled information systems: SCI and HEA

OCIO's Technical Standard and Guideline IT-930-03, *Security Assessment and Authorization*, dated December 2016, 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 decision that those risks are at an acceptable level for SI. The assessment and authorization process culminates in an official authorization to operate, which is issued for one to three years depending on the risk level of the system. When the authorization to operate expires, the system must undergo the authorization process again.

Williams Adley found that SAO's assessment and authorization packages, which are used to document the controls and underpin the assessment process, for the SCI and HEA systems expired in FY 2013. As of the end of FY 2017, OCIO was still working to address an open audit recommendation, which recommended that OCIO improve its security assessment and authorization process.[8] Part of the response to that recommendation included re-authorizing all information systems. During the FY 2017 audit, Williams Adley confirmed that SAO was working with OCIO to re-authorize both systems.

(5) SAO did not track and resolve information security weaknesses in the two sampled systems (SCI and HEA) within established target dates

SI policy requires that the system security officer "…tracks progress of implementation of their system's POA&Ms in meeting milestones and remediation actions and …" as part of the reporting to OCIO, "note if POA&Ms are on schedule and identify any missed milestones and the cause of the delay."[9] For FY 2017, Williams Adley tested 100 percent (16[10] of 16) of SAO's POA&Ms for the HEA (13 total) and SCI (3 total) systems to determine if the SAO managed the POA&Ms in accordance with its policy.

[8] Smithsonian OIG, *Fiscal Year 2015 Independent Evaluation of the Smithsonian Institution's Information Security Program, Report Number OIG-A-16-11*, September 30, 2016.

[9] Office of the Chief Information Officer, Technical Standard & Guideline IT-930-03, *Security Assessment & Authorization*, revised December 2016.

[10] POA&M list collected October 2017.

Williams Adley found that all 16 POA&Ms were overdue at the time the testing was performed, in October 2017. Specifically, for the SCI system, one of three was due in FY 2014, and two of three were due in FY 2015; for the HEA system, three of 13 were due in FY 2014, eight of 13 were due in FY 2015, and two of 13 did not have an identified due date. In fact, there was no information documented as part of the POA&Ms' status to explain the delay for all 16 overdue POA&Ms.

By not maintaining accurate information in POA&Ms,[11] OCIO and SAO lacked the information needed to effectively assess the risk posed by information security weaknesses in SAO systems.

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 three subfunctions: configuration management, identity and access management, and security training.

In FY 2017, the Protect function operated at maturity Level 2: Defined. To be effective, DHS requires a function to be at least at Level 4: Managed and Measurable. The assessed maturity level reflects improvements in two of three subfunctions—identity and access management, and security training—both of which progressed to maturity Level 2: Defined. The third subfunction, configuration management, was assessed at maturity Level 1: Ad-hoc.

Configuration Management

Information systems are constantly changing in response to updated hardware, new software capabilities, or patches to correct software flaws. The implementation of such changes may require adjustments to be made to the system configuration. Configuration management is a collection of activities focused on establishing and maintaining the integrity of information systems by controlling 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 process must consider the security implications when determining how to implement the necessary changes.

In FY 2017, SI's configuration management program was at Level 1: Ad-hoc. This low maturity level resulted primarily from OCIO's out-of-date configuration management standard, which was last updated in 2003, and a lack of documented configuration management procedures for the two systems selected for testing: SAO's SCI and HEA systems.

[11] This process involves planning and monitoring corrective actions to ensure the most critical information security weaknesses with the greatest potential impact on the entity's systems are addressed first; recognizing that resource limitations often prevent the mitigation of all identified weaknesses within the same time period. Therefore, a POA&M details the risks posed by information security weaknesses (high, medium, low), resources (time and costs) required to remediate them, any milestones in meeting the task objectives, and scheduled completion dates for the milestones.

Entity-level

(1) OCIO's configuration management policy has not been updated since 2003, despite a requirement to update it at least every three years

OCIO's Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, control CM-01, states: "the organization reviews and updates the current configuration management policy at least every 3 years and configuration management procedures at least every 3 years." Williams Adley requested the current configuration management plan, policies, and procedures from OCIO. The document provided—Technical Standard and Guideline IT-920-03, *Configuration Management*—was last updated in March 2003.

OCIO management was aware of the out-of-date standard and planned to make updates during FY 2018. While OCIO did provide Williams Adley with several technical notes[12] surrounding configuration management, IT-920-03 is the key configuration management policy outlining the process to conduct and document changes to SI information systems. In particular, the out-of-date policy does not reflect changes to NIST 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, which was published in August 2011 and specifically addresses the configuration management process.

System-level

(2) SAO did not establish a Change Control Board to manage changes in the SCI and HEA systems

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, CM-03, states, "the organization audits and reviews activities associated with configuration-controlled changes to the information system; and coordinates and provides oversight for configuration change control activities through a configuration change control committee or board that convenes when proposed changes need to be reviewed/approved." Williams Adley inquired with SAO personnel and was informed that SAO did not have a Change Control Board (CCB) that can review and approve changes to the SCI and HEA systems. Without a CCB, changes may be made to SAO systems without being properly authorized, reviewed, and tested for their impact on the systems' operations and security. OCIO and SAO management do not believe that SAO needs a formal CCB.

(3) SAO did not have fully documented and implemented configuration management plans for the SCI and HEA systems

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, CM-09, states,

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

> *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.*

A documented and implemented configuration management plan keeps system settings secure and prevents unauthorized changes to the system. Williams Adley requested and reviewed the configuration plans for SAO's SCI and HEA systems.

SCI System

Williams Adley was informed by the SAO Information Technology Director that SCI did not have a documented configuration management plan; however, OCIO's Director of Information Technology Security provided a configuration management plan for the SCI system. Williams Adley followed up with the personnel responsible for managing the SCI system and determined that they were not aware of the configuration management plan provided by OCIO for their system. As a result, they did not implement a formal configuration management process during FY 2017.

Although OCIO's configuration management plan was not used for the SCI system, Williams Adley reviewed the plan to determine if it contained the required information as documented in the *Security Controls Manual*. The SCI configuration management plan stated, "responsibilities of the [configuration management] CM staff are to establish, develop, test, implement, and maintain secured baselines that not only conform to SI policy security requirements but also meet the required business functionality." Williams Adley noted that the roles were not described in sufficient detail to determine individual responsibilities. Williams Adley also noted that the plan did not include policies and procedures for identifying and controlling configurable settings.

HEA System

The SAO provided Williams Adley with the HEA system's configuration management plan. Williams Adley noted that the plan did not define roles and responsibilities as required. In addition, the plan lacked documented policies and procedures for identifying configuration items and for placing configuration items under configuration management.

(4) SAO did not have documented policies and procedures for establishing baseline system configurations for the SCI and HEA systems

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, CM-02, states, "The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system." Baseline configurations are specifications for a system that have been formally reviewed and agreed on. The specifications are used to ensure consistent and secure installation of software across the entity. During FY 2017, Williams Adley determined that the SAO did not have a documented process for creating baseline configurations of the SCI and HEA systems.

Specifically, although OCIO has established baselines at the entity level, the SAO has not established system-specific baselines for the SCI and HEA systems. Williams Adley reached this conclusion by inquiring with OCIO management about the process for establishing and implementing baseline configurations in the SCI and HEA systems. If a process is not in place, then system baselines cannot be established, which was exactly what Williams Adley found during our review of the SCI and HEA systems' configuration management plan.

(5) SAO did not have documented policies and procedures for identifying and remediating vulnerabilities in the SCI and HEA systems, leading to a lack of vulnerability scanning

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, RA-05, requires the organization to use scanning tools that identify and enumerate system vulnerabilities and then to remediate the vulnerabilities based on risk. OCIO defines policies and procedures; however, based on interviews with SAO staff, Williams Adley determined that the SAO did not implement these policies and procedures. Instead, SAO followed an informal vulnerability management process in an ad-hoc manner for both the SCI and HEA systems.

To determine if SAO remediated flaws, despite not having documented policies and procedures, Williams Adley requested three monthly vulnerability scans: December 2016, January 2017, and February 2017. SAO was unable to provide any scan results for the three months, and did not provide an explanation as to why the scans were not performed. As a result, Williams Adley determined that vulnerability scanning was not conducted for FY 2017.

(6) SAO did not fully implement a change management log for the SCI system

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, CM-03 section "e" requires that the organization maintain a record of configuration-controlled changes to the information system for 18 months. OCIO's change management plan requires a change management log to document the details of changes, including the name of the person requesting the change, date submitted, date approved, and status of the change.

Williams Adley requested and received the FY 2017 change management log for the SCI system. Williams Adley noted that the log did not list the name of the requestor or the status. While the log contained dates for each change, it did not specify if that was the submission date or the approval date. In addition, changes were not tracked to ensure consistency, correctness, and completeness within the log. For example, Williams Adley requested the supporting documentation for four of the 108 documented changes. SAO provided Williams Adley with incomplete documentation (e.g., emails among team members), which included only patching information. The log provided to Williams Adley did not contain justification, evaluation, testing results, or official approval as required by the SCI configuration management plan.

Identity and Access Management

Effective access control processes are critical in preventing unauthorized dissemination or modification of data because they ensure 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, by internal employees or by external attackers, endangering the confidentiality, integrity, and availability of SI systems.

In FY 2017, Williams Adley found that SI had improved identity and access management by (1) implementing an automated process to remove inactive user accounts and (2) documenting and starting a review process for privileged users. Given the improvements, SI's identity and access management was assessed at Level 2: Defined. However, SI had not progressed to the next maturity level due to processes that remain at Level 1: Ad-hoc, both at the program level and within the two systems selected for testing.

Entity-level

(1) OCIO did not have documented policies and procedures in place for separation of duties

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, AC-05,[13] requires that the "organization separates administrative roles, documents separation of duties of individuals, and defines information system access authorizations to support separation of duties." Separation of duties, along with the principle of least privilege, reduces the potential for abuse of authorized privileges and reduces the risk of malevolent activity without collusion.

Williams Adley's review of OCIO's information security policies and procedures found that OCIO did not have guidance to assist system owners in establishing and implementing segregation of duties requirements. This includes both documenting separation of duties for individuals and documenting information system access authorizations to support the separation of duties. Williams Adley made follow-up inquiries to determine if separation of duties practices were in place, even if they were undocumented, and determined that there was no process or segregation of duties matrix to ensure users within SI do not have conflicting administrative roles.

System-level

(2) SAO did not have a fully documented process to onboard, modify, and offboard users for the two SAO information systems reviewed

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, AC-01 part 2, requires the organization to develop "Procedures to facilitate the implementation of the access control policy and associated access controls." Williams Adley

[13] Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, July 2017.

requested the procedures related to onboarding, modification, and offboarding of users for SAO's SCI and HEA systems, but SAO was unable to provide written procedures. According to SAO IT management, the process to onboard, modify, and offboard users is by verbal discussion and use of its internal website. Williams Adley reviewed the website and determined that it was used to make requests for access, but did not provide detailed instructions for support staff to fulfill the requests. Without such guidance, users may be provided with access that is not appropriate for their job responsibilities or may retain access that is no longer needed.

(3) SAO did not document a process to periodically review user access for the two SAO information systems reviewed, as required by OCIO policies

As stated in Technote IT-930-TN37, each system must have a documented process for managing accounts that includes a process to periodically review accounts at least quarterly and to modify or deactivate accounts as appropriate. Williams Adley inquired with SAO IT management to determine how access reviews were performed. SAO IT management informed Williams Adley that a review was completed in FY 2017 for the SCI system, but that the procedures for performing the review were not documented. SAO IT management provided incomplete evidence of an access review for the HEA system, which did not have documented procedures for conducting the review. Specifically, eight of the 10 user reviews were not fully completed.

(4) SAO did not document separation of duties for individuals for SCI and HEA systems

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, AC-05, requires that the separation of duties of individuals be documented and that the information system access authorizations to support the separation of duties be documented. Separation of duties, along with the principle of least privilege, reduces the potential for abuse of authorized privileges and reduces the risk of malevolent activity without collusion. Williams Adley inquired of key IT personnel who support the SCI and HEA systems and were informed that separation of duties was not documented.

Security Training

People are often the weakest link in security. Security 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. 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 FY 2017, OCIO improved security training by updating its entity-wide specialized security training program, testing staff with periodic phishing emails, and analyzing test results to identify areas for improvement. OCIO also received an above 90 percent completion rate for the number of users completing the required training in a timely manner. OCIO also had dashboards that showed the state of compliance of all personnel, from the end user to executive management. A monthly security awareness newsletter is sent to all SI personnel and other security awareness communications are sent periodically; personnel also participate in National

Cyber Security Awareness Month (NCSAM). Given the improvements, Williams Adley assessed the Security Training program at Level 2: Defined. However, Williams Adley noted that management had not documented a strategy to guide future improvements in the information security training program.

Entity-level

(1) OCIO did not have a long-term strategy to guide future improvements in information security training

NIST 800-50[14] 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. It 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." Williams Adley requested a copy of the FY 2017 security training strategy, and was informed by OCIO management that there was no long-term strategy documented at the time of the request. OCIO management personnel stated that they were satisfied with the status of the security training and did not see the benefit of creating a long-term strategy to move the program forward. OCIO management also stated that it continually looks to improve security training and set annual goals. Without a long-term strategy guided by a needs assessment, OCIO's limited training resources may not be targeting the most significant skill gaps.

III. Detect

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

In FY 2017, OCIO improved the Detect function by strengthening the ISCM program. Given the improvements, Williams Adley assessed the area as Level 2: Defined. Although SI is making progress in maturing the Detect function, there remain areas within continuous monitoring that have not progressed beyond Level 1: Ad-hoc.

Information Security Continuous Monitoring

ISCM enables an entity to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[15] 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. In addition, OCIO

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

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

would be unable to produce the key security metrics needed to measure and monitor the effectiveness of its current information security posture.[16]

In FY 2017, OCIO improved the maturity of its ISCM program to Level 2: Defined, by defining and beginning to implement an ISCM strategy. However, OCIO had not fully implemented its ISCM strategy by the fiscal year end to have an effective ISCM program.

Entity-level

(1) OCIO did not fully implement the ISCM strategy according to their implementation plan

The ISCM implementation plan documented within the strategy was divided into four phases, with an overall completion date of July 2, 2018. At the time of Williams Adley's testing in October 2017, Phase One was scheduled for completion, with a target of June 5, 2017, as well as several milestones within Phase Two. Williams Adley reviewed OCIO's progress in meeting these milestones and found that the following three areas were overdue:

(a) Fully implement metrics identified within the ISCM strategy by March 27, 2017.

Williams Adley inspected OCIO's monitoring dashboard and noted that OCIO had not fully implemented all metrics identified in the ISCM strategy by the end of FY 2017. OCIO management personnel stated that there were challenges in identifying source data in some cases; in other cases, OCIO had not yet identified a solution for how to monitor metrics. In addition, SI was unable to fully use the metrics for its ISCM strategy. As stated in the ISCM strategy, metrics are organized into meaningful information to support decision-making and reporting requirements. Metrics include information acquired at different frequencies and calculated from a combination of security status monitoring, from security control assessment data, and from data collected from one or more security controls. However, as of fiscal year end, OCIO had not documented a monitoring process for metrics that were implemented.

(b) Fully implement an ongoing assessment and authorization process for its information systems by March 27, 2017.

OCIO encountered delays in implementing the ongoing assessment and authorization process, including implementation of the assessment and authorization system, adding required security controls to the systems, and gathering all the data and documentation required to support the system's assessment. As a result, OCIO had completed re-authorization of only four of an estimated 48 major systems and programs by the end of the fiscal year. The reauthorization process can take several weeks to a few months for each system; thus, it will take time and effort to complete the project. Williams Adley

[16] 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.

noted that the re-authorization was not completed for the two systems selected for testing—SAO SCI and SAO HEA—but both were slated for completion by December 2017.

(c) Document procedures to support the ISCM strategy and respond to alerts by May 5, 2017.

The strategy states that policies and procedures to support the ISCM program will be documented. NIST 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, requires the following, "Policy for modifications to and maintenance of the monitoring strategy; Policy and procedures for implementation and use of organization-wide tools; Policy and procedures for establishment of monitoring frequencies; Policy and procedures for security status monitoring; and Policy and procedures for security status reporting (on control effectiveness and status monitoring)." As of September 30, 2017, OCIO had implemented some aspects of the ISCM strategy, such as identifying some key metrics and creating a dashboard that monitors some of the identified key metrics. However, OCIO had not yet documented policies and procedures for the monitoring and use of metrics or how to respond to alerts.

System-level

(2) OCIO did not define an ISCM program for SAO's SCI and HEA systems

OCIO's ISCM strategy[17] stated that all SI information systems should be included in the ISCM program. However, at the end of FY 2017, OCIO had limited visibility into the SAO systems and had not coordinated with SAO management to monitor its systems. For example, Williams Adley noted that although OCIO performed limited website vulnerability scanning for SAO, the SAO did not provide OCIO with access to scan the SCI and HEA systems for vulnerabilities. If OCIO does not have sufficient visibility into the SCI and HEA systems, then OCIO's ISCM program cannot be fully effective, and separate provisions would be needed for the SCI and HEA systems.

(3) SAO did not conduct vulnerability scanning on the SAO SCI and SAO HEA systems

SI Technote IT-930-TN33, *Vulnerability Management Program*, states: "all assets connected to the Smithsonian networks (public and private), including those operated on behalf of the Smithsonian that are externally hosted, are scanned on schedule and/or on request and/or [on an] as needed basis such as a release of external security advisories such as those received from US-CERT [United States Computer Emergency Readiness Team]." The scanning schedule for major systems, which include the SCI and HEA systems, was documented as weekly. Williams Adley requested vulnerability scans for the months of December 2016, January 2017, and February 2017, but SAO was unable to provide the scan results for any of the weeks within the three

[17] *Smithsonian Institution Information Security Continuous Monitoring Strategy.*

requested months. Also, as noted above, SAO not only did not use the centralized vulnerability scanning services provided by OCIO, but also did not develop its own procedures to implement the IT-930-TN33 policy requirements for the vulnerability scanning process.

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 Technote 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 the Smithsonian's ability to perform its mission."

In FY 2017, the Respond function had progressed from maturity Level 1: Ad-hoc in FY 2016 to Level 2: Defined. This process matured because OCIO invested resources in adopting and configuring a centralized Security Information and Event Management (SIEM) tool[18] and adopting a Governance, Risk, and Compliance (GRC) tool.[19] As a result, most of the Incident Response process was documented, but not yet being consistently implemented.[20]

Incident Response:

Technote IT-930-TN30 states "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." In addition, 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 FY 2017, a major portion of the incident response program was documented, meaning that the policies and procedures were established, but there were still three of seven incident response requirements at maturity Level 1: Ad-hoc. For example, SI had not yet fully implemented the SIEM tool to monitor and alert security staff when a potential security incident is detected. In addition, although the program is formally documented in policy, it lacks key areas required by NIST guidance and has not been updated to incorporate the new US-CERT requirements. Also, certain areas with documented policies and procedures (e.g., prioritizing incidents and reporting incidents to US-CERT) were not consistently implemented.

Another example of how incident response shortfalls affected SI during FY 2017 are apparent in a security breach that occurred in SAO's HEA system. SAO's Incident Response Plan stipulates that an incident classified as unauthorized access must be reported to OCIO within 1 hour of identification, to US-CERT within 1 hour, and to the individuals affected by the loss of personally identifiable information (PII) within 24 hours of identification. On November 5, 2016, a security incident occurred when the HEA system was breached. SAO staff did not discover the incident until November 7, 2016, and did not report the incident to OCIO until November 10,

[18] A SIEM tool provides analysis of security alerts generated by applications and network hardware to help stop cybersecurity threats.

[19] A GRC tool synchronizes information and activity across governance, risk management, and compliance.

[20] To move from Level 1 to Level 2, at least 50 percent of the Level 1 metrics must be met, unless they are not applicable to the entity.

2016. OCIO did not report the incident to US-CERT until November 15, 2016. By that time, the intruders had downloaded PII for more than 1,000 researchers, including names, addresses, and phone numbers. This was further compounded by the fact that SAO and OCIO were unaware that the system contained PII until November 17, and then took another 11 days (November 28) to notify the affected individuals.

Entity-level

(1) OCIO did not fully configure the SIEM tool to support the incident response program

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, 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." Williams Adley was informed by OCIO management that the SIEM tool did not provide meaningful and actionable information by the end of FY 2017 due to the number of false positive alerts it generated. While it was not fully implemented, the configuration of the SIEM tool is an extensive and complicated process that OCIO continued throughout 2017. OCIO estimated that the configuration would be ongoing throughout FY 2018.

(2) OCIO did not have fully documented plans, policies, and procedures that incorporated current guidance from NIST and US-CERT, as required

Williams Adley reviewed OCIO's IT Security Incident Response Procedures[21] and noted that seven areas required by NIST were not documented. Specifically, the following were not formally documented in a policy, procedure, or plan: (1) identification of major incidents; (2) incident response correlation[22]; (3) insider threat program[23]; (4) common threat vector taxonomy[24]; (5) metrics for measuring the incident response capability and effectiveness;[25] (6) roadmap for maturing the incident response capability[26]; and (7) how the program fits within the overall organization.[27]

In addition, SI did not use the US-CERT [28] reporting requirements from April 1, 2017, to update the incident reporting timeframes. Specifically, the last revised date on Technote IT-930-TN30 was January 6, 2015. As of September 30, 2017, SI used categorizations based on the type of incident (i.e., Category 1: Unauthorized Access; Category 2: Denial of Service), which aligned

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

[22] 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.

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

[24] 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.

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

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

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

[28] 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.

with outdated US-CERT requirements; these categorizations do not prioritize a security incident's criticality.

Current US-CERT categorizations, released October 2014 and required by September 30, 2015, depict the level of Functional Impact (high, medium, low, none), Information Impact (classified, proprietary, privacy, integrity, none), and Recoverability (regular, supplemented, extended, not recoverable, not applicable) to better assess the impact of the incident on the environment. If security incidents are not managed based on potential impact, then a serious incident might not be addressed before others that are less critical.

(3) OCIO did not implement a documented process to prioritize incidents

OCIO's *IT Security Incident Response Procedures*, Technote IT-930-TN30, requires the Security Operations Center (SOC) to categorize reported incidents as part of the incident assessment to assist in prioritizing the incident. Williams Adley reviewed eight of 53 security incident tracking tickets (Heat Ticket). Testing results showed that while each ticket had a field titled "priority," the field for all eight tickets stated that "this field isn't required." OCIO management personnel stated that there is no process in place to determine the priority of security incidents. Also, when a new security incident occurs, it becomes a priority over the existing open incidents. If a priority or criticality is not assigned for incidents, then low-risk incidents might be addressed before high-risk incidents, based solely on the timing of the incidents, which increases the risk to the information system by potentially not addressing the highest risk security incidents first.

(4) OCIO did not report incidents in accordance with the documented timeframes

While SI had established procedures for incident response,[29] Williams Adley noted that OCIO did not report all security incidents to US-CERT[30] within the SI-mandated timeframe. OCIO's *IT Security Incident Response Procedures* Technote IT-930-TN30, requires reporting to US-CERT within specified timeframes according to incident categorization. Williams Adley reviewed all 53 incidents reported in FY 2017, and selected eight of those incidents for detailed testing. Williams Adley's test results identified the following issues:

- 40 of 53 incidents, marked Category 1–6, were not reported to US-CERT. Policy requires that each incident be submitted within 4 hours or at least within 1 month, depending on the category.
- One Category 1 incident (Heat Ticket 1214568) was not reported to the OIG. Policy requires that all Category 1 incidents be reported to the OIG.
- Two of eight Category 1 incidents were not reported within the required 4-hour timeframe:

[29] Office of the Chief Information Officer, SI Technote IT-930-TN30, *IT Security Incident Response Procedures*, Internal Smithsonian Policy, revised January 2015

[30] 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.

- Heat Ticket 1158059 was detected by the SOC on November 10, 2016, but was not reported to US-CERT until November 15, 2016.
- Heat Ticket 1178531 was detected by the SOC on February 4, 2017, but was not reported to US-CERT until February 6, 2017.

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 FY 2017, the Recover function was assessed at Level 1: Ad-hoc, which is the lowest maturity rating on the scale from one to five. Although SI is taking steps to improve the Recover function, there remain significant shortfalls that prevent SI from reaching the next maturity level.

Contingency Planning

The primary purpose of contingency planning is to prepare for rare events that have the potential for significant consequences and to escalate addressing first-priority risks. 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 natural disasters, can result in competing priorities with respect to recovery efforts. If there has not been sufficient planning, prioritization decisions must be made in real time without the benefit of deliberate analysis, which likely will result in errors, rework, and delayed recovery.

In FY 2017, SI took steps to improve its contingency planning program. For example, OCIO participated in the Smithsonian Emergency Management Advisory Committee to create, enhance, and maintain the Smithsonian Emergency Management Program. OCIO also continued to conduct its annual disaster recovery testing for Enterprise Resource Planning (ERP) systems, financial systems, and human resources systems. However, Williams Adley found that contingency planning was operating at Level 1: Ad-hoc because OCIO did not have updated disaster recovery planning guidance and the SAO did not have an information system contingency plan. In addition, the SAO did not have documented backup and recovery policies and procedures for the two information systems tested.

Entity-level

(1) OCIO continued to rely on outdated policies and procedures to support its IT contingency planning program during 2017

During the prior year's audit of SI's information security program (FY 2016), Williams Adley noted that OCIO had not updated its Technical Standard & Guideline IT-960-02 *Disaster Recovery Planning* since 2003. Williams Adley recommended updating the document to reflect current NIST guidance. OCIO agreed and established a target date of June 30, 2019. As a result, OCIO's guidance to support its IT contingency planning program remained outdated during FY 2017.

(2) OCIO did not define an entity-wide disaster recovery plan[31] based on a business impact analysis[32]

According to NIST 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, a disaster recovery plan should be based on a business impact analysis that identifies key business processes and related information systems. Using the business impact analysis to guide the disaster recovery plan, the organization can prioritize recovery of the most critical systems.

When Williams Adley requested the entity-wide IT disaster recovery plan, OCIO provided a plan that focused primarily on a few key ERP systems. The plan lacked the key information required to align information system contingency plans across the SI organization to ensure information systems and procedures are identified and prioritized during recovery to minimize organizational downtime. Also, the plan was not based on any business impact analysis results because an analysis had not been conducted by the end of FY 2017. According to OCIO management, a business impact analysis would be beneficial, but it must be conducted at the SI recovery planning level.

System-level

(3) SAO did not develop an information system contingency plan[33] for the two sampled systems: SCI and HEA

Information Technology Technical Standards & Guidelines IT-930-02, *Security Controls Manual Version 4.1*, CP-02, requires that the organization develop a contingency plan for each information system. It requires that the plan address key information such as essential missions and business functions associated with contingency requirements; recovery objectives, restoration priorities, and metrics; contingency roles, responsibilities, and assigned individuals with contact information; and full information system restoration.

Williams Adley requested the recovery plan for the SAO's SCI and HEA systems. SAO IT staff provided a draft copy of a recovery plan from FY 2013, but the plan was neither finalized nor formally signed. Also, there were highlights in the recovery plan indicating missing information and there were question marks indicating unanswered questions. As a result, Williams Adley determined that the document was incomplete.

[31] The disaster recovery plan (DRP) provides procedures for relocating information systems operations to an alternate location. Thorough recovery strategies ensure that the entity's information systems may be recovered quickly and effectively following a disruption.

[32] The business impact analyses (BIA) helps identify and prioritize information systems and components critical to supporting the entity's business processes.

[33] The information system contingency plan (ISCP) should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

(4) SAO management did not formally test or train in recovery procedures

SI policy requires annual testing of each information system's contingency plan.[34] This testing includes failover or tabletop tests, reviews of the test results, and development of corrective actions, if necessary. Williams Adley requested the most recent test results for the SCI and HEA systems. However, SAO IT management informed Williams Adley that it did not test or train staff in recovery procedures. Management also stated that SAO performed only limited testing of the system recovery when bringing systems online after a scheduled power outage. Williams Adley determined that this type of testing did not meet SI policy requirements. If recovery procedures are not fully tested, system recovery after a disaster may be significantly delayed.

(5) SAO did not define backup and data recovery policies and procedures for the SCI and HEA systems

SAO is required to maintain its own backup and recovery policies and procedures per SI Technote IT-960-TN46, *Backup and Data Recovery.*[35] When Williams Adley requested SAO's backup and recovery policies and procedures, SAO IT management was able to provide only a backup schedule that documented the system files to be archived. This schedule did not include documented policies and procedures on critical areas such as frequency of backups, backup policy for each type of data, backup media, and a documented process for data recovery. Without documented policies and procedures for backup and recovery, SAO IT management may be unable to recover its systems and/or data.

Conclusion

In FY 2017 OCIO established and took additional steps to implement key elements of SI's information security program. OCIO prioritized resources to address identified deficiencies, including implementation of a governance, risk, and compliance tool, and initiating the re-authorization of all information systems. These two projects are labor and resource intensive, which led to other projects being delayed.

Despite these activities, Williams Adley determined that SI's information security program did not achieve the minimum maturity level necessary to be considered fully effective. To further mature the information security program, SI must continue to develop policies and procedures and to consistently implement them. Williams Adley provided the following recommendations to help SI enhance its information security program:

[34] IT-930-02 control CP-04

[35] IT-960-TN46 states that, "the owner of systems, applications, websites, and data hosted on servers, in consultation with OCIO, specifies backup schedule and policy to be performed by OCIO or unit IT support staff, or performs backup and recovery of files for own servers."

Recommendations

Identify
Recommendation 1: Williams Adley recommends that the Chief Information Officer ensure that the SAO continuously monitor and update POA&Ms in accordance with Technical Standard & Guideline IT-930-03 Security Assessment & Authorization.

Recommendation 2: Williams Adley recommends that the Chief Information Officer expand the minimum required data for the inventory of information system components to better ensure the availability of data that may be needed in response to an incident.

Protect
Recommendation 3: Williams Adley recommends that the Chief Information Officer update the entity-level configuration management policy, in accordance with National Institute of Standards and Technology Special Publication 800-53 Revision 4.

Recommendation 4: Williams Adley recommends that the Chief Information Officer ensure that the SAO implement a system-level Change Control Board in accordance with Technical Standard & Guideline IT-930-02 to oversee changes at the system level.

Detect
Recommendation 5: Williams Adley recommends that the Chief Information Officer collaborate with SAO system owners to ensure appropriate access is granted to OCIO personnel to conduct continuous monitoring activities on the SAO information systems.

Recommendation 6: Williams Adley recommends that the Chief Information Officer ensure that the SAO develop policies and procedures to conduct vulnerability scans of its environment and allow centralized scans.

Respond
Recommendation 7: Williams Adley recommends that the Chief Information Officer update the incident response plan to reflect changes in National Institute of Standards and Technology Special Publication 800-61 Revision 2 and the United States Computer Emergency Readiness Team reporting guidance.

Recover
Recommendation 8: Williams Adley recommends that the Chief Information Officer conduct a business impact analysis to correlate the information systems with the critical mission processes and services provided and, based on that information, characterize the consequences of a disruption, in accordance with National Institute of Standards and Technology Special Publication 800-34 Revision 1.

Recommendation 9: Williams Adley recommends that the Chief Information Officer ensure that the SAO develop information system contingency plans, including policies and procedures on backups and recovery, for the SAO Scientific Computing Infrastructure and HEA information systems, in accordance with National Institute of Standards and Technology Special Publication 800-34 Revision 1.

Appendix A – Guidance

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

Office of Management and Budget (OMB) 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. 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. Smithsonian Institution's 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 Actions 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

Incident Response

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

VI. 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

Appendix B – Smithsonian OIG's Fiscal Year 2017 Submission to CyberScope

Overall	
FISMA Question	**FY 2017 Assessment**
0.1 - Please provide an overall IG self-assessment rating (Effective/Not Effective).	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 Smithsonian Institution systems, Smithsonian Astrophysical Observatory (SAO) Scientific Computing Infrastructure (SCI) and SAO High Energy Astrophysics (HEA), to perform detailed testing for the FY 2017 FISMA audit. Based on our inquiry with Smithsonian Institution personnel and inspection of the supporting documentation, Smithsonian Institution has not fully developed strategies and plans for most FISMA domains. In addition, Smithsonian Institution has not fully defined information security related policies and procedures for the in-scope systems. The Department of Homeland Security considers Level 4, *Managed and Measurable*, as an effective level of overall security program. Based on the assessment of Smithsonian Institution's information security program, the overall maturity level results in-between Level 1, *Ad-hoc,* and Level 2, *Defined*.

Function: Identify – Risk Management	
FISMA Question	**FY 2017 Assessment**
1 - 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 and PM-5; OMB M-04-25; NIST	**Level 2: Defined** – Smithsonian Institution is in the process to fully identify and maintain a comprehensive and accurate inventory of its information systems. This inventory is expected to be completed by December 2017.

Cybersecurity Framework (CSF): ID.AM-1 – 4)?	
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)?	**Level 1: Ad-Hoc** – Smithsonian Institution maintains a hardware inventory, however, Williams Adley was not provided with policies and procedures that outline how the inventory is maintained and what key attributes (taxonomy) are required.
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, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?	**Level 1: Ad-Hoc** – Smithsonian Institution maintains a software inventory, however, Williams Adley was not provided with policies and procedures that outline how the inventory is maintained and what key attributes (taxonomy) are required.
4 - To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?	**Level 1: Ad-Hoc** – Smithsonian Institution is in the process of re-categorizing and communicating the importance of information systems in enabling its missions and business functions.
5 - To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk,	**Level 1: Ad-Hoc** – Smithsonian Institution has implemented policies and procedures for risk management at the system-level. However, there is no defined entity or business level risk management strategy. The entity-wide risk management strategy and implementation plan, policies, and procedures are being developed.

and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?	
6 - Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization 's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?	**Level 1: Ad-Hoc** – Smithsonian Institution has defined its information security monitoring program; however, it is not fully implemented. Additionally, the hardware and software inventory management process has not been defined.
7 - To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, 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 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?	**Level 1: Ad-Hoc** – Smithsonian Institution has defined roles and responsibilities at the system-level and identified a Chief Risk Executive to lead the entity-wide risk management program. However, the entity-wide risk management strategy and implementation plan, policies, and procedures are in the process of being developed.
8 - To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?	**Level 2: Defined** – Smithsonian Institution has implemented the use of POA&Ms; however, Smithsonian Institution is in the process of transitioning between POA&M tools. In addition, POA&Ms for Smithsonian Astrophysical Observatory (SAO) systems, Scientific Computing Infrastructure (SCI) and High Energy Astrophysics (HEA), were not remediated in a timely manner.
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	**Level 2: Defined** – Smithsonian Institution has defined Information Security Risk Assessment procedures which includes threats, vulnerabilities, and impacts. However, the risk assessment procedures have not been fully implemented.

(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) 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)?	
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)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not define how information about risks are communicated in a timely manner to all necessary internal and external stakeholders.
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 Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract	**Level 2: Defined** – Smithsonian Institution has developed policies and procedures that require a memorandum of understanding and interconnection security agreement to be completed. Additionally, there is a standard privacy and security clause that is required.

Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?	
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 began implementation of a tool, Archer, to provide a centralized view of risks across the entity's information systems. However, the Archer tool and associated metrics and usage have not been fully implemented.
13.1 - Please provide the assessed maturity level for the agency's Identify - Risk Management function.	**Level 1:** Ad-Hoc
13.2 - 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*, as an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall risk management program is at the ad-hoc level.
Calculated Maturity Level	**Level 1: Ad-Hoc**

Function: Protect – Configuration Management	
FISMA Question	**FY 2017 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.

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 1: Ad-Hoc** – Smithsonian Institution did not fully define a configuration management plan.
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 1: Ad-Hoc** – Smithsonian Institution has defined configuration management policies and procedures. However, Williams Adley was not provided with SAO SCI and SAO HEA configuration management policies and procedures.
17 - To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not fully define baseline configurations policies and procedures at the system-level.
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 1: Ad-Hoc** – Smithsonian Institution did not fully define baseline configurations at the system-level.

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 1: Ad-Hoc** – Smithsonian Institution did not fully define flaw remediation processes to manage software vulnerabilities at the system-level.
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 1: Ad-Hoc** – Smithsonian Institution chose not to adopt the TIC program.
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 CCB, as appropriate (NIST 800-53: CM--2, CM-3)?	**Level 1: Ad-Hoc** – Smithsonian Institution has not fully defined and implemented configuration change control activities, including auditing and review of configuration changes and oversight of changes implemented.
22 - Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions	The Department of Homeland Security considers Level 4, *Managed and Measurable*, as an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall configuration management program is at the ad-hoc level.

above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?	
Calculated Maturity Level	**Level 1: Ad-Hoc**

Function: Protect – Identity & Access Management	
FISMA Question	**FY 2017 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 1: Ad-Hoc** – Smithsonian Institution did not define a strategy to guide its identity and access management 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 1: Ad-hoc** - Smithsonian Institution has not fully defined policies and procedures for identity and access management across the organization.
26 - To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53:	**Level 2: Defined** – Smithsonian Institution has developed and defined procedures for screening and assigning personnel risk designations.

PS-2, PS- 3; and National Insider Threat Policy)?	
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 access agreements for users and privileged users.
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 1: Ad-Hoc** – Smithsonian Institution has chosen not to implement PIV.
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 1: Ad-Hoc** – Smithsonian Institution has chosen not to implement PIV.
30 - To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and	**Level 1: Ad-Hoc –** Smithsonian Institution has defined a process to perform quarterly review of privileged access. However, the review is being performed annually. In addition, Smithsonian Institution, including SAO, did not perform a review of privileged users' activity logs.

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 appropriate configuration requirements implemented for remote access connections. However, Smithsonian Institution did not log or review remote activities based on risk.
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*, as an effective level of 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 – Security Training	
FISMA Question	**FY 2017 Assessment**
33 - 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 800-53: AT-1; and NIST SP 800-50)?	**Level 2: Defined –** Smithsonian Institution has defined roles and responsibilities of security awareness and training program stakeholders.
34 - 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 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?	**Level 2: Defined –** Smithsonian Institution does not have a formalized skill and gap assessment program. However, individual units assess training requirements per individual is conducted each year.
35 - 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	**Level 1: Ad-Hoc –** Smithsonian Institution did not define a security awareness and training strategy that focuses on the following components: organizational priorities, goals of the program, use of technology, and deployment methods.

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 800--53: AT-1; NIST 800-50: Section 3))	
36 - 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 questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)	**Level 2: Defined** – Smithsonian Institution has defined security awareness and specialized security training policies and procedures.
37 - 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 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)	**Level 2: Defined** – Smithsonian Institution has defined its processes for ensuring that all information system users are provided security awareness training within 30 days of being granted system access. However, Smithsonian Institution did not define its processes for evaluating and obtaining feedback of its security awareness and training program for continuous improvements.
38 - To what degree does the organization ensure that specialized security training is provided to all individuals with significant	**Level 2: Defined** – Smithsonian Institution has defined specialized security training.

security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?	
39.1 - Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).	**Level 2: Defined**
39.2 - 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*, as an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall security training program is at the defined level.
Calculated Maturity Level	**Level 2: Defined**

Function: Detect – Information Security Continuous Monitoring	
FISMA Question	**FY 2017 Assessment**
40 - 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 and began the communication and implementation of an ISCM strategy. The implementation plan will continue into FY 2018.
41 - 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	**Level 1: Ad-Hoc** – Smithsonian Institution did not develop and implement information security continuous monitoring policies and procedures to support the ISCM strategy.

and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting 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 43)	
42 - 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 2017 CIO FISMA Metrics)?	**Level 2: Defined** – Smithsonian Institution has defined the key stakeholders' roles and responsibilities in the ISCM strategy.
43 - How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?	**Level 2: Defined** – Smithsonian Institution has developed the ongoing assessment process for system authorization and monitoring security controls. However, it is planned to be implemented in FY 2018.
44 - How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?	**Level 1: Ad-Hoc** – Smithsonian Institution has completed a list of metrics for tracking purposes. However, the metrics are not being fully collected or monitored for completion. Additionally, the metrics do not have a defined monitoring frequency.
45.1 - Please provide the assessed maturity level for the agency's Detect - ISCM function.	**Level 2: Defined**
45.2 - Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted	The Department of Homeland Security considers Level 4, *Managed and Measurable*, as an effective level of overall security program. Based on our

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?	testing, Williams Adley determined that Smithsonian Institution's overall ISCM program is at the defined level.
Calculated Maturity Level	**Level 2: Defined**

Function: Respond – Incident Response	
FISMA Question	**FY 2017 Assessment**
46 - 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 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)	**Level 2: Defined** – Smithsonian Institution has not fully defined and implemented its incident response policies and procedures. The policies and procedures do not include: incident response planning, considerations for major incidents, incident response testing, incident response correlation, and insider threat handling for incident response.
47 - To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?	**Level 2: Defined** – Smithsonian Institution has defined and communicated the structures of its incident response teams, roles, and responsibilities of incident response stakeholders, and associated levels of authority and dependencies.
48 - 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; US- CERT Incident Response Guidelines)?	**Level 1: Ad-Hoc** – Smithsonian Institution has not fully configured the Security Information and Event Management (SIEM) tool. In addition, there is no defined threat vector taxonomy.

49 - How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?	**Level 1: Ad-Hoc**– Smithsonian Institution has not updated their incident handling procedures to reflect the latest US-CERT guidelines. Additionally, major incidents are not defined and containment strategies for specific types of incidents are not defined.
50 - 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-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?	**Level 2: Defined** – Smithsonian Institution has defined its requirements for personnel to report suspected security incidents to the entity's help desk and/or security operations center within the defined timeframes. In addition, Smithsonian Institution has defined its processes for reporting security incidents to US-CERT.
51 - 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 and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not define guidelines on how to collaborate with stakeholders to ensure on-site technical assistance can be leveraged for quickly responding to incidents. In addition, Smithsonian Institution did not implement the Department of Homeland Security's Einstein program.
52 - 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*	**Level 2: Defined**– Smithsonian Institution has implemented many of these tools to support the incident response program.

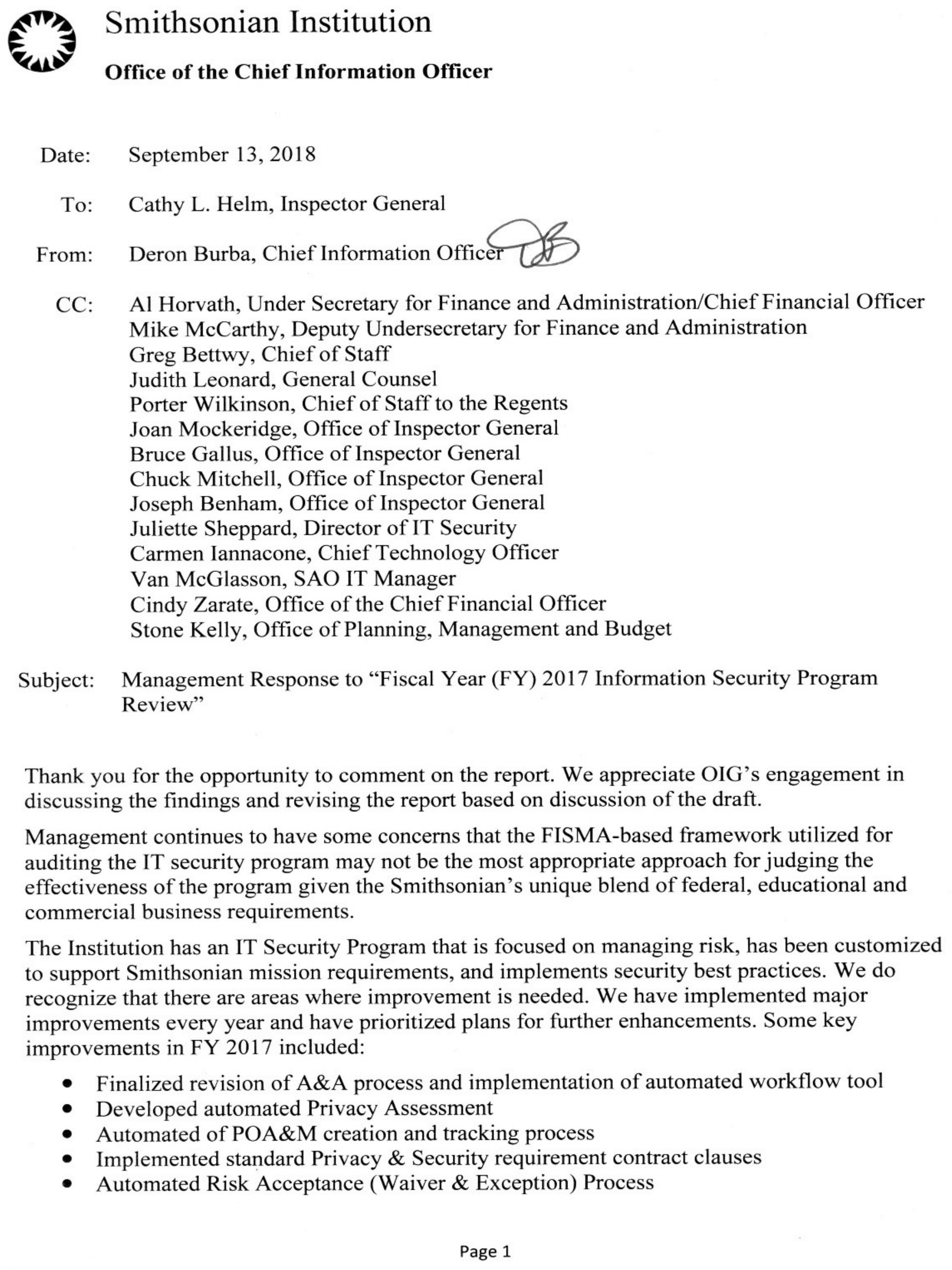
- Information management, such as data loss prevention *- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)*	
53.1 - Please provide the assessed maturity level for the agency's Respond - Incident Response function.	**Level 2: Defined**
53.2 - Provide any 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*, as an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall incident response program is at the defined level.
Calculated Maturity Level	**Level 2: Defined**

Function: Recover – Contingency Planning	
FISMA Question	**FY 2017 Assessment**
54 - 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 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not define information system contingency planning program.
55 - 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	**Level 1: Ad-Hoc** – Smithsonian Institution did not define information system contingency planning program.

should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800--161).	
56 - To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not define a process for conducting a business impact analyses nor conducted a business impact analyses to guide contingency planning efforts.
57 - To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not define policies and procedures for developing information system contingency plans. In addition, Williams Adley was not provided with SAO SCI and SAO HEA information system contingency plans.
58 - To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?	**Level 1: Ad-Hoc** – Williams Adley was not provided with SAO SCI and SAO HEA information system contingency plans. There were no official test or training completed in FY 2017, however when power is shut off in the building, SAO staff use the opportunity to practice recovery procedures.
59 - To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR. IP- 4; and NARA guidance on information systems security records)?	**Level 1: Ad-Hoc** – Smithsonian Institution has defined system backup and storage processes. However, Williams Adley was not provided with defined system backup procedures for SAO SCI and SAO HEA.
60 - 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 800-53: CP-2, IR-4)?	**Level 1: Ad-Hoc** – Smithsonian Institution did not fully define recovery activities efforts. In addition, Smithsonian Institution did not conduct a Business Impact Analyses.

61.1 - Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.	**Level 1: Ad-Hoc**
61.2 - 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*, as an effective level of overall security program. Based on our testing, Williams Adley determined that Smithsonian Institution's overall contingency planning program is at the ad-hoc level.
Calculated Maturity Level	**Level 1: Ad-Hoc**

Appendix C – Management's Response



Smithsonian Institution

Office of the Chief Information Officer

Date: September 13, 2018

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer

CC: Al Horvath, Under Secretary for Finance and Administration/Chief Financial Officer
Mike McCarthy, Deputy 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
Bruce Gallus, Office of Inspector General
Chuck Mitchell, Office of Inspector General
Joseph Benham, Office of Inspector General
Juliette Sheppard, Director of IT Security
Carmen Iannacone, Chief Technology Officer
Van McGlasson, SAO IT Manager
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

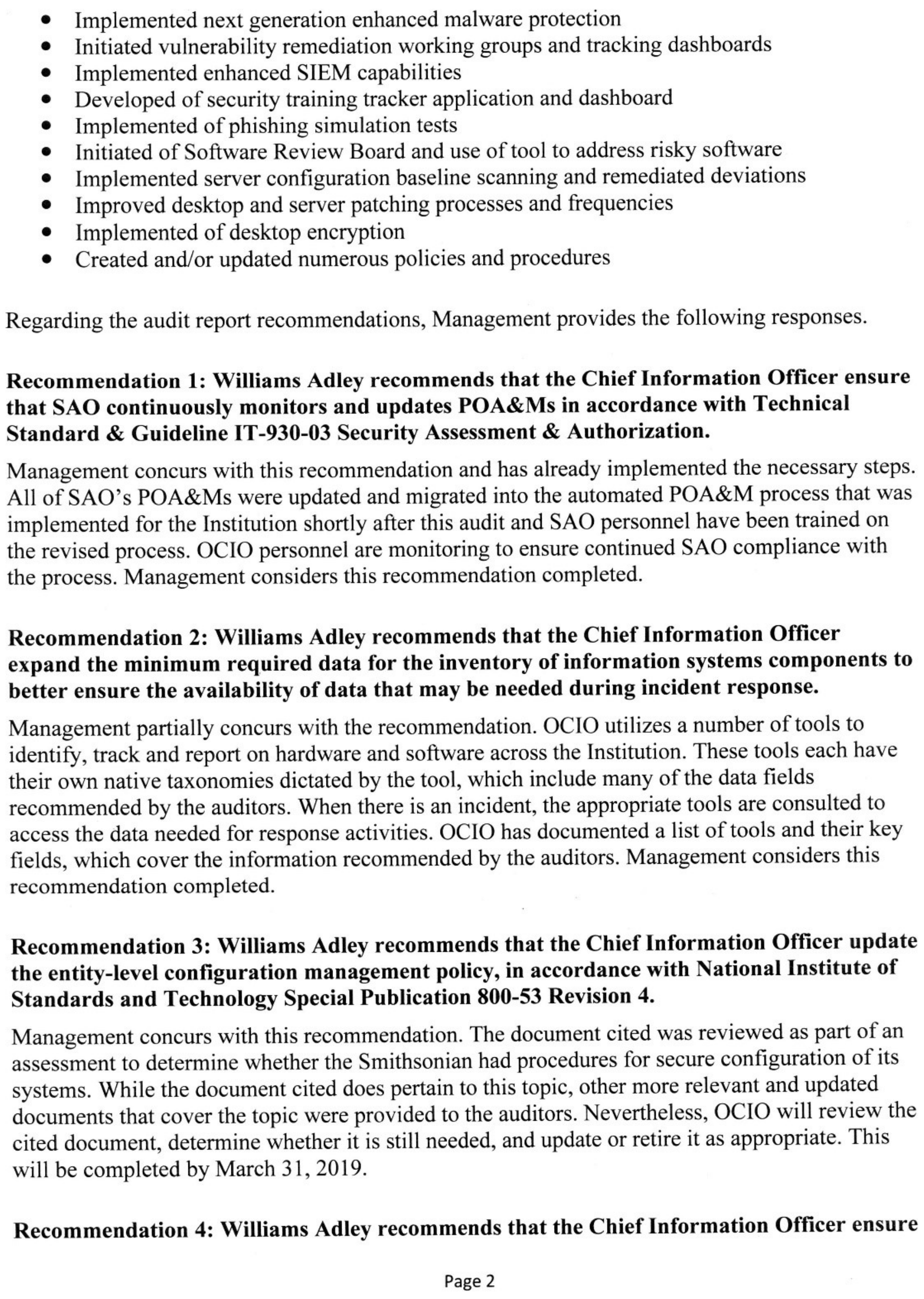
Subject: Management Response to "Fiscal Year (FY) 2017 Information Security Program Review"

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.

Management continues to have some concerns that the FISMA-based framework utilized for auditing the IT security program may not be the most appropriate approach for judging the effectiveness of the program given the Smithsonian's unique blend of federal, educational and commercial business requirements.

The Institution has an IT Security Program that is focused on managing risk, has been customized to support Smithsonian mission requirements, and implements security best practices. We do recognize that there are areas where improvement is needed. We have implemented major improvements every year and have prioritized plans for further enhancements. Some key improvements in FY 2017 included:

- Finalized revision of A&A process and implementation of automated workflow tool
- Developed automated Privacy Assessment
- Automated of POA&M creation and tracking process
- Implemented standard Privacy & Security requirement contract clauses
- Automated Risk Acceptance (Waiver & Exception) Process



- Implemented next generation enhanced malware protection
- Initiated vulnerability remediation working groups and tracking dashboards
- Implemented enhanced SIEM capabilities
- Developed of security training tracker application and dashboard
- Implemented of phishing simulation tests
- Initiated of Software Review Board and use of tool to address risky software
- Implemented server configuration baseline scanning and remediated deviations
- Improved desktop and server patching processes and frequencies
- Implemented of desktop encryption
- Created and/or updated numerous policies and procedures

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

Recommendation 1: Williams Adley recommends that the Chief Information Officer ensure that SAO continuously monitors and updates POA&Ms in accordance with Technical Standard & Guideline IT-930-03 Security Assessment & Authorization.

Management concurs with this recommendation and has already implemented the necessary steps. All of SAO's POA&Ms were updated and migrated into the automated POA&M process that was implemented for the Institution shortly after this audit and SAO personnel have been trained on the revised process. OCIO personnel are monitoring to ensure continued SAO compliance with the process. Management considers this recommendation completed.

Recommendation 2: Williams Adley recommends that the Chief Information Officer expand the minimum required data for the inventory of information systems components to better ensure the availability of data that may be needed during incident response.

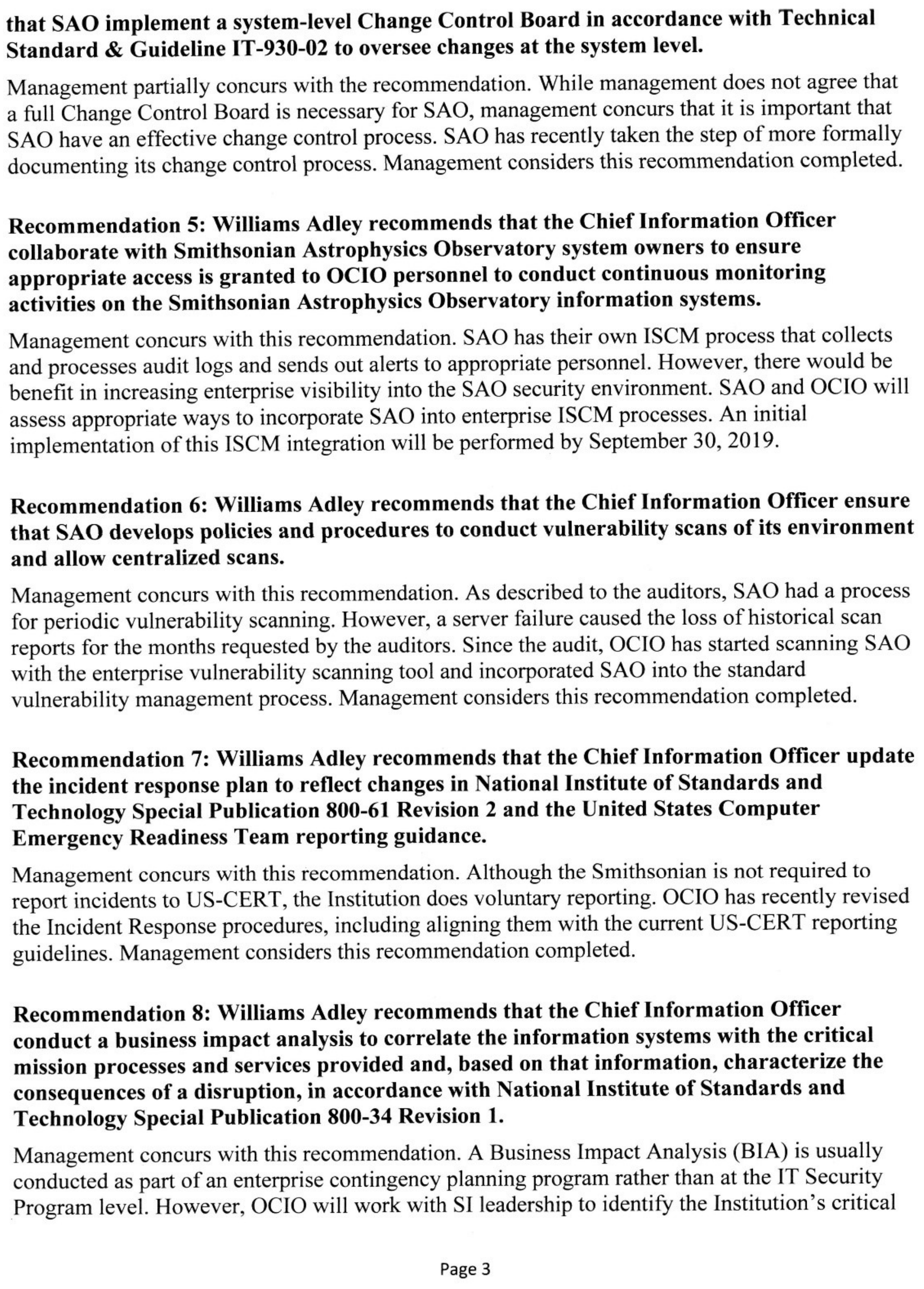
Management partially concurs with the recommendation. OCIO utilizes a number of tools to identify, track and report on hardware and software across the Institution. These tools each have their own native taxonomies dictated by the tool, which include many of the data fields recommended by the auditors. When there is an incident, the appropriate tools are consulted to access the data needed for response activities. OCIO has documented a list of tools and their key fields, which cover the information recommended by the auditors. Management considers this recommendation completed.

Recommendation 3: Williams Adley recommends that the Chief Information Officer update the entity-level configuration management policy, in accordance with National Institute of Standards and Technology Special Publication 800-53 Revision 4.

Management concurs with this recommendation. The document cited was reviewed as part of an assessment to determine whether the Smithsonian had procedures for secure configuration of its systems. While the document cited does pertain to this topic, other more relevant and updated documents that cover the topic were provided to the auditors. Nevertheless, OCIO will review the cited document, determine whether it is still needed, and update or retire it as appropriate. This will be completed by March 31, 2019.

Recommendation 4: Williams Adley recommends that the Chief Information Officer ensure

Page 2



that SAO implement a system-level Change Control Board in accordance with Technical Standard & Guideline IT-930-02 to oversee changes at the system level.

Management partially concurs with the recommendation. While management does not agree that a full Change Control Board is necessary for SAO, management concurs that it is important that SAO have an effective change control process. SAO has recently taken the step of more formally documenting its change control process. Management considers this recommendation completed.

Recommendation 5: Williams Adley recommends that the Chief Information Officer collaborate with Smithsonian Astrophysics Observatory system owners to ensure appropriate access is granted to OCIO personnel to conduct continuous monitoring activities on the Smithsonian Astrophysics Observatory information systems.

Management concurs with this recommendation. SAO has their own ISCM process that collects and processes audit logs and sends out alerts to appropriate personnel. However, there would be benefit in increasing enterprise visibility into the SAO security environment. SAO and OCIO will assess appropriate ways to incorporate SAO into enterprise ISCM processes. An initial implementation of this ISCM integration will be performed by September 30, 2019.

Recommendation 6: Williams Adley recommends that the Chief Information Officer ensure that SAO develops policies and procedures to conduct vulnerability scans of its environment and allow centralized scans.

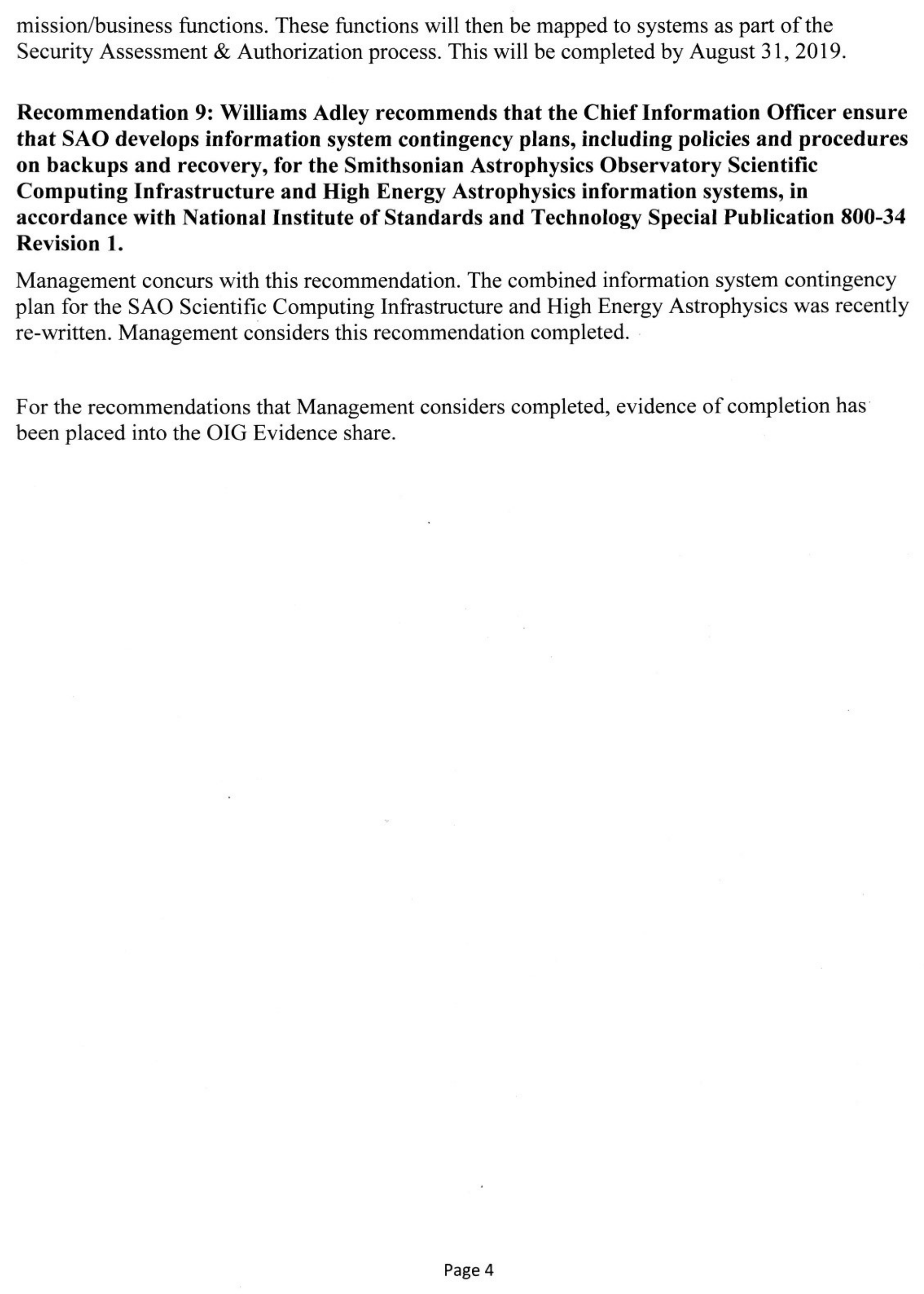
Management concurs with this recommendation. As described to the auditors, SAO had a process for periodic vulnerability scanning. However, a server failure caused the loss of historical scan reports for the months requested by the auditors. Since the audit, OCIO has started scanning SAO with the enterprise vulnerability scanning tool and incorporated SAO into the standard vulnerability management process. Management considers this recommendation completed.

Recommendation 7: Williams Adley recommends that the Chief Information Officer update the incident response plan to reflect changes in National Institute of Standards and Technology Special Publication 800-61 Revision 2 and the United States Computer Emergency Readiness Team reporting guidance.

Management concurs with this recommendation. Although the Smithsonian is not required to report incidents to US-CERT, the Institution does voluntary reporting. OCIO has recently revised the Incident Response procedures, including aligning them with the current US-CERT reporting guidelines. Management considers this recommendation completed.

Recommendation 8: Williams Adley recommends that the Chief Information Officer conduct a business impact analysis to correlate the information systems with the critical mission processes and services provided and, based on that information, characterize the consequences of a disruption, in accordance with National Institute of Standards and Technology Special Publication 800-34 Revision 1.

Management concurs with this recommendation. A Business Impact Analysis (BIA) is usually conducted as part of an enterprise contingency planning program rather than at the IT Security Program level. However, OCIO will work with SI leadership to identify the Institution's critical



mission/business functions. These functions will then be mapped to systems as part of the Security Assessment & Authorization process. This will be completed by August 31, 2019.

Recommendation 9: Williams Adley recommends that the Chief Information Officer ensure that SAO develops information system contingency plans, including policies and procedures on backups and recovery, for the Smithsonian Astrophysics Observatory Scientific Computing Infrastructure and High Energy Astrophysics information systems, in accordance with National Institute of Standards and Technology Special Publication 800-34 Revision 1.

Management concurs with this recommendation. The combined information system contingency plan for the SAO Scientific Computing Infrastructure and High Energy Astrophysics was recently re-written. Management considers this recommendation completed.

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