



In Brief

Fiscal Year 2016 Independent Evaluation of the Smithsonian Institution's Information Security Program

OIG-A-18-02, November 21, 2017

What OIG Did

The Smithsonian's 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 2016 and to support the Office of the Inspector General's annual report under FISMA.

Background

FISMA was enacted in 2002 to strengthen the security of the federal government's information systems. Although the Smithsonian is not subject to FISMA because it is not an executive branch agency, the Smithsonian applies FISMA standards as best practices to the extent practicable and consistent with its mission.

FISMA requires organizations to adopt a risk-based, life cycle approach to improving information security that includes annual security program reviews, independent Office of Inspector General evaluations, and reporting to the Department of Homeland Security and the Congress.

What Was Found

For fiscal year 2016, the Office of the Chief Information Officer (OCIO) implemented key elements of the Smithsonian Institution's (Smithsonian) information security program. For example, OCIO had policies for vulnerability management, incident response, configuration management, and security training. However, an independent public accounting firm, Williams, Adley & Company – DC, LLP (Williams Adley), found that OCIO did not have an effective risk-based process to target resources with the highest risk vulnerabilities for the two information systems tested. One of the two systems provides the network infrastructure for most of the Smithsonian.

In addition, OCIO had neither established nor implemented an enterprise information security architecture to ensure that information technology security processes are effectively deployed to secure the Smithsonian's operating environment. Furthermore, by end of fiscal year 2016, OCIO had not resolved significant issues found in prior audits, such as the overdue implementation of an information security continuous monitoring program that helps assess the ongoing risks in the information security environment. OCIO had a target date of December 2016 to begin implementing such a program.

Based on the deficiencies found during this audit and the significant unresolved issues from prior audits, Williams Adley determined that the Smithsonian did not meet its information security program goals. In addition, the Smithsonian was operating at the lowest Federal Information Security Modernization Act (FISMA) metrics maturity level—Level 1: Ad hoc—for two of the five FISMA cybersecurity framework security functions, Detect and Respond. As a result, the Smithsonian's information security program was not fully effective in reducing information security risks in fiscal year 2016.

What Was Recommended

Williams Adley made three recommendations to enhance information security at the Smithsonian. Management concurred with two of the three recommendations and partially concurred with the third recommendation. For the partially concurred recommendation, management agreed with the key aspects of the recommendation and provided an explanation for why it could not be applied in all cases.



Smithsonian Institution

Office of the Inspector General

Memo

Date: November 21, 2017

To: David J. Skorton, Secretary

Cc: Albert Horvath, Under Secretary for Finance and Administration and Chief Financial Officer (OUSF&A)


Greg Bettwy, Chief of Staff, Office of the Secretary

Porter N. Wilkinson, Chief of Staff to the Board of Regents

Cindy Zarate, Executive Officer, OUSF&A

Deron Burba, Chief Information Officer

Juliette Sheppard, Director, Information Technology Security

From: Cathy L. Helm, Inspector General 

Subject: Fiscal Year 2016 Evaluation of the Smithsonian Institution's Information Security Program (OIG-A-18-02)

This memorandum transmits Williams, Adley & Company - DC, LLP's (Williams Adley) final report on the fiscal year 2016 evaluation of the Smithsonian Institution's (Smithsonian) information security program. The Federal Information Security Modernization Act (FISMA) requires an annual evaluation, by the Inspector General, of the security of federal information systems. The Smithsonian is not required to comply with FISMA because it is not an executive branch agency. However in fiscal year 2016, the Smithsonian applied FISMA standards as best practices to the extent practicable and consistent with its mission.

Under a contract monitored by this office, the Office of the Inspector General (OIG) engaged Williams Adley, an independent public accounting firm, to perform the audit. Williams Adley found that for fiscal year 2016, the Office of the Chief Information Officer (OCIO) implemented key elements of the Smithsonian's information security program. However, Williams Adley also found that OCIO did not have an effective risk-based process to target resources with the highest risk vulnerabilities for the two information systems tested. Management concurred with two of Williams Adley's three recommendations, partially concurred with the third recommendation, 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

**Smithsonian Institution
Office of Inspector General**

Report on the Smithsonian Institution's Information Security Program

Fiscal Year 2016

November 21, 2017





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, 2016.

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-17-05 ("*Fiscal Year 2016-2017 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 2016 FISMA audit report. Their response is included in the recommendation section of this report, and 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. 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
Washington, District of Columbia
November 21, 2017

WILLIAMS, ADLEY & COMPANY-DC, LLP

Management Consultants/Certified Public Accountants

1030 15th Street, NW, Suite 350 West • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161

Smithsonian Institution
FY 2016 Information Security Program Review

Contents

Abbreviations	3
Introduction	4
Purpose	4
Objectives, Scope and Methodology	5
I. Objective	5
II. Scope and Methodology	5
Background	6
I. The Smithsonian Institution	6
II. The Office of the Chief Information Officer	6
III. Federal Information Security Modernization Act of 2014	6
IV. SI IT Security Program Plan	9
Results in Brief	11
Results of Audit	11
I. Risk Management	11
II. Vulnerability Management	15
III. Enterprise Security Architecture	16
IV. Incident Management	16
V. Contingency Plans	17
VI. Access Control Processes	18
VII. Baseline Configurations	18
Conclusion	19
Recommendations	19
Appendix A – Guidance	20
Appendix B – Status of Prior Years’ Findings & Recommendations, as of November 20, 2017	22
Appendix C – Management’s Response	27

Smithsonian Institution
FY 2016 Information Security Program Review

Abbreviations

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
FISMA	Federal Information Security Modernization Act
FMS	Facility Management System
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
Institution	Smithsonian Institution
ISCM	Information Security Continuous Monitoring
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PCI DSS	Payment Card Industry Data Security Standard
POA&M	Plan of Action and Milestones
SD	Smithsonian Directive
SI	Smithsonian Institution
SINet	Smithsonian Institution's Network
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
VOIP	Voice Over Internet Protocol

Smithsonian Institution
FY 2016 Information Security Program Review

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).

SI is not required to comply with FISMA because it is not an executive branch agency. However, SI applies FISMA standards as best practices to the extent practicable and consistent with its mission. For the fiscal year (FY) 2016 review, Williams Adley used SI's Information Technology (IT) Security Program Plan and OIG FISMA CyberScope metrics to determine the status of SI's information security program.

SI's IT Security Program Plan was designed using National Institute of Standards and Technology (NIST) and FISMA guidance. The IT Security Program Plan is divided into seven control areas: Risk Management, Vulnerability Management, Enterprise Security Architecture, Incident Management, Security Education Training and Awareness, Contingency Planning, and Security Policies.

The FY 2016 FISMA CyberScope metrics consist of five cybersecurity framework security functions: Identify, Protect, Detect, Respond, and Recover. These five functions are comprised of eight areas: Risk Management, Contractor Systems, Identity & Access Management, Configuration Management, Security & Privacy Training, Information Security Continuous Monitoring (ISCM), Incident Response, and Contingency Planning. The Department of Homeland Security (DHS) uses the FISMA CyberScope metrics to determine an entity's information security program level. The levels range from Level 1: Ad hoc to Level 5: Optimized. DHS considers an information security program at Level 4: Managed and Measurable to be an effective information security program.

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 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.

Smithsonian Institution
FY 2016 Information Security Program Review

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. The audit was performed in accordance with Office of Management and Budget (OMB) reporting guidance¹ and covered the period October 1, 2015, to September 30, 2016 (FY 2016).

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: Smithsonian Institution Network (SINet) and Facility Management System (FMS).

SINet is the general support system that supports the computing infrastructure and core services used by SI employees and affiliated persons² to perform their daily work. These services include Internet, telephone, email remote access, content filtering, file storage, and other services that are integral to operating an entity the size of SI. Access to the SI network is granted through login to SINet. Security controls for FMS and other applications are inherited from SINet.

FMS manages the physical security within the structures of SI. FMS is composed of five subsystems: FacilityCenter, Visit Count Management System, Security Incident Response System, Parking Management System, and SI Explorer.

The Smithsonian OIG contracted Williams Adley to assess the effectiveness of SI's information security program and practices. Williams Adley performed the audit from August 2016 through October 2016 in accordance with *Generally Accepted Government Auditing Standards* (GAGAS). GAGAS requires that Williams Adley plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the review objectives. Williams Adley believes the evidence obtained provides a reasonable basis for the findings and conclusions based on the review objectives.

To perform this audit, Williams Adley interviewed SI management, employees, and contractors to evaluate the effectiveness of SI's information security program in accordance with NIST and OMB guidance. Williams Adley also observed daily operations, conducted judgmental sampling where applicable, inspected SI policies and procedures to supplement observations and interviews, and obtained sufficient evidence to support our conclusions and recommendations. Furthermore, Williams Adley reviewed system-generated outputs (e.g., active directory listings) where possible to support our conclusions.

¹ Office of Management and Budget (OMB), *Fiscal Year 2016–2017 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-17-05, November 4, 2016.

² The Smithsonian defines the following as affiliated persons: contractors, volunteers, researchers, students, interns, fellows, Friends of the National Zoo employees, Smithsonian Early Enrichment Center employees, and Smithsonian Associates educators.

Smithsonian Institution
FY 2016 Information Security Program Review

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. 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. OCIO reports to SI's Undersecretary of Finance and Administration/Chief Financial Officer.

III. Federal Information Security Modernization Act of 2014

Through the Federal Information Security Management Act of 2002,³ as amended by the Federal Information Security Modernization Act of 2014,⁴ 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 entities, 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 fiscal year's reporting requirements.⁵ 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.

For FY 2016, FISMA consisted of five cybersecurity framework security functions: identify, protect, detect, respond, and recover. The five FISMA cybersecurity framework security functions consist of eight metric domains, 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

³ *E-Government Act of 2002*, Public Law 107-347, December 17, 2002.

⁴ *Federal Information Security Modernization Act of 2014*, Public Law 113-283, December 18, 2014.

⁵ OMB, *Fiscal Year 2016–2017 Guidance on Federal Information Security and Privacy Management Requirements*, Memorandum M-17-05, November 4, 2016.

Smithsonian Institution
FY 2016 Information Security Program Review

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.

- Contractor Systems – The contractor systems management process ensures that information systems operated by contractors and other external entities on behalf of the federal government meet all applicable security 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 can help security managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their responsibility, thus enabling managers to direct changes as required. The goal of configuration management is to make assets harder to exploit through better configuration.
- Vulnerability management, an aspect of configuration management, focuses on the detection and elimination of software and hardware vulnerabilities. Detection is performed by scanning the network using tools that test for vulnerabilities. Once vulnerabilities are discovered, software patches can be appropriately configured, tested, and implemented.
- Identity and Access Management – The primary purpose of identity and access management is to establish a process to ensure users and devices are authenticated⁶ 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 authorization⁷ to access information and information systems.
- Security and Privacy Training – Establishing and maintaining a robust and relevant information security training process as part of the overall information security program is the primary conduit for providing a workforce with the information and tools needed to protect an agency's vital information resources. This training helps ensure that personnel at all levels of the entity understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Entities that continually train their workforce in organizational security policy and role-

⁶ The process of identifying an individual, usually based on a username and password.

⁷ Authorization allows the user to access various resources based on the user's identity, which is authenticated with a username and password.

Smithsonian Institution
FY 2016 Information Security Program Review

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 either intentional 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.

For FY 2016, FISMA implemented a maturity model for two of the five FISMA cybersecurity framework security functions, Detect and Respond, to help determine the level of development and implementation for each entity. These maturity model ratings are as follows:

- Level 1: Ad hoc – The program is not formalized and activities are performed in a reactive manner, resulting in an ad hoc program.
- Level 2: Defined – The program is formalized through the development of comprehensive policies, procedures, and strategies consistent with NIST, OMB, and United States Computer Emergency Readiness Team (US-CERT) requirements. However, the policies, procedures, and strategies are not consistently implemented entity-wide.
- Level 3: Consistently Implemented – The entity consistently implements its program across the entity. However, qualitative and quantitative measures and data on the effectiveness of the program across the entity are not captured and used to make risk-based decisions.
- Level 4: Managed & Measurable – Program activities are repeatable and metrics are used to measure and manage implementation of the program, achieve situational awareness, and control ongoing risk. DHS considers Level 4: Managed and Measurable an effective information security program.
- Level 5: Optimized – The entity's program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business or mission requirements and a changing threat and technology landscape.

Smithsonian Institution
FY 2016 Information Security Program Review

These ratings are based on a series of 9–12 questions per level that are to be answered by the OIG or entity. The questions revolve around the use and implementation of people, processes, and technologies. To move from Level 1 to Level 2, an entity must have answered yes to all Level 1 questions unless they are not applicable to the entity. For example, SI has decided not to implement personal identity verification (PIV) cards and a trusted Internet connection (TIC). The fact that PIV and TIC were not implemented in the SI environment was not considered when determining SI's level of information security.

The remaining three of the five FISMA cybersecurity framework security functions use maturity indicators to assess the current information security posture. These three areas are Identify, Protect, and Recover. The assessment is completed by answering a series of FISMA CyberScope questions that indicate the maturity level. The same maturity ratings described above are used; however, the questions are not as comprehensive as the maturity model and give only an indication of the probable maturity level.

IV. SI IT Security Program Plan

The IT Security Program Plan was published in 2014 to provide guidance to SI as it designed and implemented an updated security program to mitigate the risks identified in the SI information systems. As stated in the IT Security Program Plan, “Without a comprehensive IT security program customized to the SI's specific needs and environment, the Institution is exposed and vulnerable to losing its ability to perform its mission, is at risk for significant financial losses, may be at risk of liability for not protecting the resources with which it has been entrusted, and risks damage to its reputation.”

The goals outlined in the IT Security Program Plan include the following:

- Facilitate cost-effective management of SI IT security risks
- Support the SI mission by protecting the availability, integrity, and confidentiality of critical information resources
- Protect the SI's image and operations by preventing and reducing the impact of security incidents
- Ensure SI's compliance with applicable information security regulations and standards.

To achieve the goals of the IT Security Program Plan, OCIO outlined several key areas of concern that must be addressed. These key areas are aligned with FISMA and NIST guidance including the following:

- IT security policies and procedures – Security policies and procedures are the foundation of good security practice. They provide the basic rules for the entity to operate securely. IT security policies and procedures are required in all FISMA cybersecurity functions.
- Security education training and awareness – Security education training and awareness ensure that everyone at SI understands not only the security policies that apply to them, but also their own role in maintaining IT security and the consequences of non-compliance. Security education training and awareness aligns with the FISMA cybersecurity function: Protect.

Smithsonian Institution
FY 2016 Information Security Program Review

- Incident management – Incident management is used to respond to a security incident that is a threat to SI information resources. Incident management aligns with the FISMA cybersecurity function: Respond.
- Vulnerability management – Vulnerability management is used to detect and address vulnerabilities to minimize risk to SI's information resources. Often vulnerabilities can be addressed by deploying the latest software patches. Vulnerability management is one part of the configuration management process. Configuration management aligns with the FISMA cybersecurity function: Protect.
- Contingency planning – Contingency plans are necessary to ensure access to critical information resources in the event of a disruption. Contingency planning aligns with the FISMA cybersecurity function: Recover.
- Enterprise security architecture – The enterprise security architecture defines a comprehensive structure for information security technologies, processes, people, and systems to ensure they are aligned to meet SI's security needs. Enterprise security architecture is a component in the domain of risk management. Risk management aligns with the FISMA cybersecurity function: Identify.
- Risk management strategies include the following:
 - System inventory and categorization – System inventory and categorization is used to ensure appropriate levels of protection are applied to information resources. System inventory and categorization is one aspect in the domain of risk management. Risk management aligns with the FISMA cybersecurity function: Identify.
 - Risk assessments – Risk assessments determine what risks exist, the likelihood of those risks occurring, and the impact if they were to occur. Risk assessment is one aspect in the domain of risk management. Risk management aligns with the FISMA cybersecurity function: Identify.
 - System security plans – System security plans provide an overview of the applicable security requirements for each information system. A system security plan is one aspect in the domain of risk management. Risk management aligns with the FISMA cybersecurity function: Identify.
 - Systems assessment and authorization – System assessment and authorization ensure that information systems have security commensurate with their level of risk. System assessment and authorization is one aspect in the domain of risk management. Risk management aligns with the FISMA cybersecurity function: Identify.
 - Information security continuous monitoring – ISCM maintains ongoing awareness of IT security, vulnerabilities, and threats to support organizational risk management decisions.⁸ Information security continuous monitoring aligns with the FISMA cybersecurity function: Detect.

Finally, the IT Security Program Plan outlines a governance structure that promotes:

- Complying with specific federal requirements and industry best practices

⁸ National Institute of Standards and Technology Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011.

Smithsonian Institution
FY 2016 Information Security Program Review

- Tracking and responding to OIG recommendations and incorporating security improvements based on OIG recommendations
- Providing timely reporting to government and other required entities on the state of SI IT security (e.g., FISMA, Payment Card Industry Data Security Standard [PCI DSS] compliance)
- Developing metrics and a dashboard to measure and reporting on the progress and effectiveness of the IT security program
- Enhancing communication about security initiatives throughout SI.

Consistent with FISMA, the IT Security Program Plan contains areas concerning Risk Management, ISCM, Incident Response, Security Training, Contingency Planning, Security Policies and Procedures, and Vulnerability Management, which is a subsection of FISMA's Configuration Management.

Results in Brief

For FY 2016, OCIO established and took steps to implement key elements of the SI's information security program. For example, OCIO had policies for vulnerability management, incident response, configuration management, and security training. However, Williams Adley found that OCIO did not have an effective risk-based process to target resources with the highest risk vulnerabilities for the two information systems tested. One of the two systems provides the network infrastructure for most of SI.

In addition, OCIO had neither established nor implemented an enterprise information security architecture to ensure that IT security processes are effectively deployed to secure SI's operating environment. Furthermore, by end of the fiscal year, OCIO had not resolved significant issues found in prior audits, such as the overdue implementation of an information security continuous monitoring program that helps assess the ongoing risks in the information security environment. OCIO had a target date of December 2016 to begin implementing such a program.

Based on the deficiencies found during this audit and the significant unresolved issues from prior audits, Williams Adley determined that SI did not meet its information security program goals and was operating at the lowest FISMA metrics maturity level—Level 1: Ad hoc—for two of the five FISMA cybersecurity framework security functions, Detect and Respond. As a result, SI's information security program was not fully effective in reducing information security risks in FY 2016. Williams Adley made three recommendations related to: Risk Management, Enterprise Security Architecture, and Disaster Recovery Planning.

Results of Audit

I. Risk Management

SI's IT Security Program Plan states that "determining a security strategy for a system or the entity, SI must determine the correct balance between mitigating risks and expending resources." Risk management is the process of identifying, assessing, mitigating, and monitoring risks. In the IT Security Program Plan, OCIO identified areas of risk management that needed to be addressed, including system inventory and categorization, information security continuous monitoring, vulnerability management, and POA&Ms. However, at the end of FY 2016, SI had

Smithsonian Institution
FY 2016 Information Security Program Review

not addressed the following risk management concerns: (1) maintain a complete and accurate inventory of SI information systems to protect information from attack; (2) adhere to its POA&M policies and procedures to ensure the most critical security weaknesses with the greatest potential impact on the entity's mission are addressed first; (3) implement an ISCM strategy to effectively monitor a dynamic IT environment; and (4) update agreements for two externally maintained contractor systems, which can contain proprietary data, to ensure information security requirements are current.

Incomplete Inventory of Information Systems

Williams Adley found that SI did not have a complete and accurate list of information systems in the SI environment in FY 2016. When asked for a list of information systems in the SI environment, OCIO provided to Williams Adley two incomplete system inventory lists. The initial list, received October 5, 2016, had 20 systems. The second list, received October 13, 2016, contained 52 additional systems⁹: two major, 49 minor, and one system that was not classified as major, minor, or general support system. One of the two sampled contractor systems, Multi-force Government Solutions/Fuel Dispenser,¹⁰ was not found on either list. OCIO managers said that the second list represented efforts to update their inventory. Furthermore, they stated that updating the information system inventory was an open recommendation from the FY 2015 IT security audit and was scheduled to be completed by December 31, 2017.

OCIO recognized the importance of a system inventory, as it is required,¹¹ and identified the need to review the information system inventory and categorize SI information systems in the IT Security Program Plan. All information systems in the SI environment must be identified as a major, minor, or general support system. In addition, SI Technote IT-930-TN34 *IT Security System Inventory* states that all systems, even minor, must be included in the system inventory. If a complete and accurate inventory is not maintained, the entity's information security program will be unable to ensure that all systems have been assessed for risk and that the risk is appropriately managed by security controls.

Plan of Action and Milestones to Address Deficiencies

In FY 2016, OCIO did not follow its policies and procedures for creating a risk-based POA&M process.¹² 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; it recognizes that resource limitations often prevent the mitigation of every identified weakness 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. By not consistently following the POA&M process, OCIO

⁹ A total of 72 systems was contained on the second information system inventory received October 13, 2016.

¹⁰ The Multi-force system allows SI to track and eventually charge for fuel usage by General Services Administration (GSA) leased vehicles.

¹¹ Office of the Chief Information Officer, Technote IT-930-TN34, *IT Security System Inventory*, Internal Smithsonian Policy, revised August 18, 2015.

¹² Office of the Chief Information Officer, Technote IT-930-TN29, *IT Security Plans of Action and Milestones*, Internal Smithsonian Policy, revised June 29, 2015.

Smithsonian Institution
FY 2016 Information Security Program Review

lacked the information needed to ensure resources were allocated to resolve the highest risk vulnerabilities first in FY 2016.

Williams Adley tested 54 POA&Ms for the two systems sampled (45 for SINet; 9 for FMS) and found that OCIO did not establish realistic completion dates for completion of POA&Ms.¹³ In fact, Williams Adley confirmed only four POA&Ms were closed and 50 remained open at the end of FY 2016. Of the four that were closed, one POA&M was closed by meeting its initial estimated completion date (2%), but the other three were closed a year after the initial estimated completion date (5%).

As illustrated in Figure 1, of the 50 open POA&Ms (42 for SINet; 8 for FMS), SI is on track to complete 22 (19 for SINet; 3 for FMS) based on their initial scheduled completion dates (41%). For the remaining 28 POA&Ms, there were 22 (17 for SINet; 5 for FMS) overdue (41%) and six (6 for SINet) had not been assigned a completion date (11%) by the end of FY 2016. In addition, of the 22 overdue POA&Ms, three were 3 years overdue, eight were 2 years overdue, six were 1 year overdue, and five were 6 months overdue.

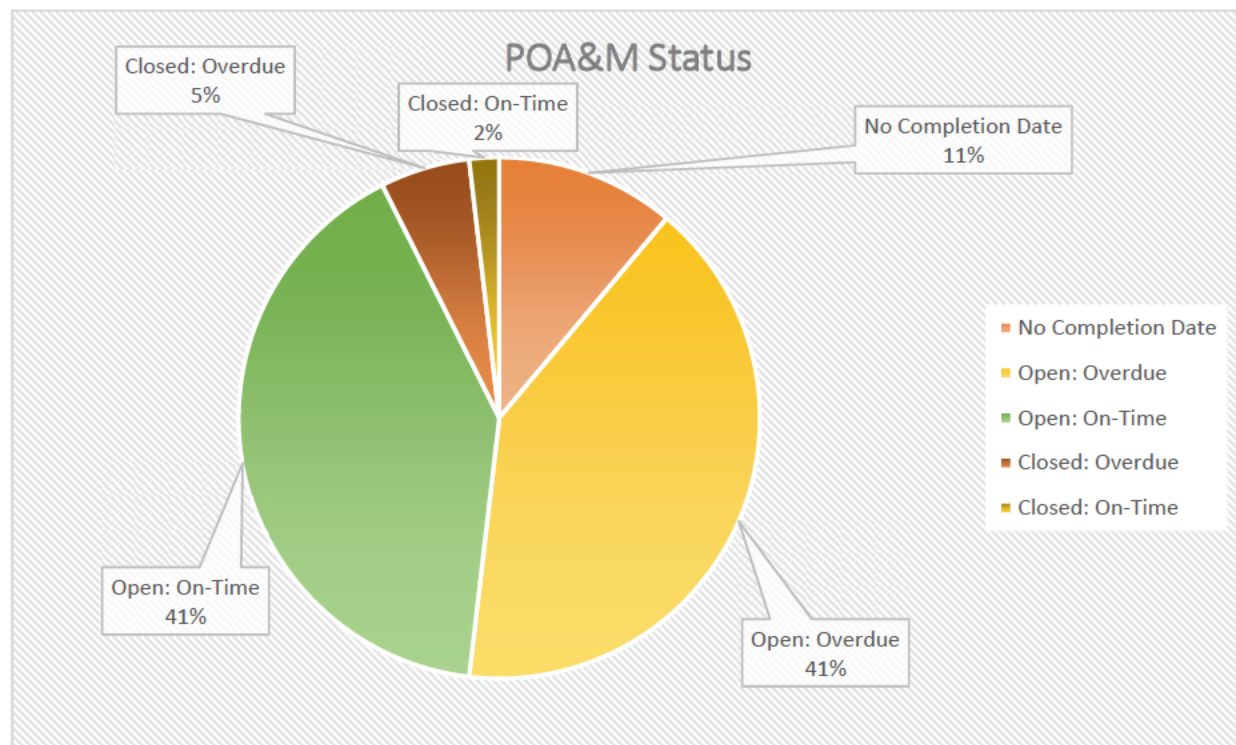


Figure 1: Status of 54 POA&Ms for Two Information Systems Selected for Testing in FY 2016, as of October 2016

SI Technote IT-930-TN29 also requires delayed POA&Ms to have details captured under milestone changes. On review of the milestone changes column in the SINet POA&M tracking sheet, Williams Adley found that OCIO did not update the milestone changes for any of the 17

¹³ POA&M list collected October 2016.

Smithsonian Institution
FY 2016 Information Security Program Review

delayed POA&Ms. Specifically, the milestone changes column was empty for all delayed SINet POA&Ms.

Finally, OCIO did not assign a risk level or resource estimate to POA&Ms, as required.¹⁴ Of the 54 tested POA&Ms:

- Thirty-four were assigned a moderate risk, 1 was assigned a low risk, and 19 were not assigned a risk level.
- Fifty-two were assigned resource estimates; two were not assigned resource estimates.

Information Security Continuous Monitoring

ISCM allows an entity to clearly understand the security state of all its information systems over time and to effectively monitor a dynamic IT environment with changing threats, vulnerabilities, technologies, business processes and functions, and critical missions. Without a fully implemented ISCM program, attempts to damage an entity's systems may result in unplanned system downtime, unauthorized access, data loss, operational failure, and unauthorized modification of data. Furthermore, without the implementation of a comprehensive ISCM program, an entity would be unable to identify the key security metrics to measure and monitor the effectiveness of its current information security posture.¹⁵

As of September 30, 2016, OCIO still did not have a defined ISCM strategy, which became a FISMA requirement in FY 2014.¹⁶ This deficiency was originally reported in the FY 2014 IT program security audit and again in the FY 2015 IT program security audit.¹⁷ This POA&M had a target date of December 2016 to begin implementation. As a result, the "Detect" cybersecurity function was defined as Level 1: Ad hoc in the FY 2016 FISMA maturity metrics. This level designates the ISCM program as not formalized and that activities are performed in a reactive manner.

Contractor Systems

Contractor systems, or external information systems, are information systems managed outside of the control of an entity. Such external systems may house and process proprietary data. Agreements should be in place to ensure these external contractor systems are managed and protected with the appropriate level of security controls.¹⁸

During the audit, Williams Adley found that one of two selected contractor systems had an interconnection security agreement that had expired in October 2014. Without an updated

¹⁴ Likelihood and impact on the information system if not addressed.

¹⁵ 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.

¹⁶ OMB, *Enhancing the Security of Federal Information and Information Systems*, Memorandum M-14-03, November 18, 2013.

¹⁷ Smithsonian OIG, *Fiscal Year 2015 Independent Evaluation of the Smithsonian Institution's Information Security Program*, Report Number OIG-1-16-11, No date.

¹⁸ Office of the Chief Information Officer, Technote IT-930-TN22, *Security Agreements for Interconnected Systems*, Internal Smithsonian Policy, revised October 17, 2006.

Smithsonian Institution
FY 2016 Information Security Program Review

agreement, OCIO may not be able to properly validate that the contractor system has implemented current information security requirements and remediated critical vulnerabilities.

As of September 30, 2016, there was an open POA&M that required the update and review of all interconnection service agreements. This POA&M has a target date of August 31, 2017.

II. Vulnerability Management

Vulnerability management, a key component of SI's information security program, is the process of identifying, classifying, and remediating software vulnerabilities. Critical-risk¹⁹ and high-risk²⁰ system vulnerabilities left unresolved provide a readily available avenue for malicious hackers. Most external information security risks are known and can be mitigated by an effective end-to-end vulnerability management program. Without effective vulnerability management, including regular patch management, an entity exposes itself to a variety of malicious attacks, including denial-of-service attacks, damage to the general support system, and exfiltration of sensitive information, including personally identifiable information (PII).

At SI, vulnerabilities are identified primarily by SD807 Ex. 2. If the vulnerability cannot be remediated, acceptance of the risk must be documented, reviewed, and approved by the Chief Information Officer (CIO). SI has policies and procedures in place that govern vulnerability management and patch management. For example, Technote IT-930-TN33 requires that a vulnerability rated as critical be remediated within SD807 Ex. 2, while a vulnerability rated high should be remediated within SD807 Ex. 2.

In FY 2016, Williams Adley reviewed SD807 Ex. 2 vulnerability scanning results for the SD807 Ex. 2 servers in SD807 Ex. 2 production environment for 3 months (July, August, September) and found that SI did not adhere to its required remediation timelines for critical- and high-risk common vulnerabilities and exposures (CVE²¹). CVEs are assigned a severity score of zero to ten using the Common Vulnerability Scoring System (CVSS) V3.0. A score of seven to eight is considered high and nine to ten is considered critical.

For SD807 Ex. 2 critical- and high-risk vulnerabilities were found in the July 2016 scan.²² Of the SD807 Ex. 2 critical- and high-risk vulnerabilities, SD807 Ex. 2 vulnerabilities that were found in July were still present in the August 2016 and September 2016 scans, despite the SI remediation requirement. Of the SD807 Ex. 2 repeated vulnerabilities, SD807 Ex. 2²³ were scored at ten, the most critical, on the CVSS.

Williams Adley found that SD807 Ex. 2 had unsupported software active in the production environment. For example, Microsoft ended security patching support for SD807 Ex. 2; however, SI still used SD807 Ex. 2 in its SD807 Ex. 2 production environment. Once software is considered unsupported, vendors are no longer guaranteed to

¹⁹ Exploitation of a critical-risk vulnerability likely results in root-level compromise of servers or infrastructure devices.

²⁰ Exploitation of high-risk vulnerability could result in elevated privileges or could result in significant data loss or downtime.

²¹ CVE is a dictionary of common vulnerability names for publicly known vulnerabilities that has been adopted worldwide.

²² Per Common Vulnerability Scoring System Version 3 (CVSS V3), a vulnerability rating of 7 to 8 is high risk; a rating of 9 to 10 is a critical risk.

²³ Of the SD807 Ex. 2 CVEs found, SD807 Ex. 2 were scored at 7 or 8; SD807 Ex. 2 were scored at 9.

Smithsonian Institution
FY 2016 Information Security Program Review

address any known or discovered vulnerabilities. As of September 30, 2016, there was an open POA&M, with a target date of July 31, 2015, to update all [REDACTED] SD807 Ex. 2

For [REDACTED] SD807 Ex. 2, Williams Adley also discovered [REDACTED] SD807 Ex. 2 high-risk vulnerabilities that were documented as POA&Ms on an [REDACTED] SD807 Ex. 2 operation server, and that had not been remediated by the end of FY 2016, even though the completion date was June 30, 2016. In addition, Williams Adley sampled 2 months of FY 2016 vulnerability reports for the [REDACTED] SD807 Ex. 2 production [REDACTED] SD807 Ex. 2 server and found [REDACTED] SD807 Ex. 2 critical-risk vulnerability, discovered in December 2015, that OCIO still had not resolved as of February 2016.

III. Enterprise Security Architecture

In FY 2016, SI did not have a defined enterprise information security architecture. As stated in the IT Security Program Plan, an enterprise information security architecture defines a comprehensive structure for information security technologies, processes, and people to ensure they align with the SI's information security needs. This includes defining the current and future state of information security to ensure it aligns with the entity's strategic plan and business requirements. It also defines the integration of all necessary security tools (e.g., intrusion detection systems, intrusion prevention systems, antivirus software, and antimalware software) and helps ensure the tools are correctly implemented within the network infrastructure. Finally, the security architecture ensures that security processes are appropriately deployed to most effectively secure the entity's operating environment.

OCIO management stated that SI did not have a defined enterprise information security architecture as of the end of FY 2016 because sufficient resources had not been allocated to complete it. Nonetheless, OCIO was aiming to finalize the ISCM portion of the enterprise information security architecture by December 31, 2016.

IV. Incident Management

As outlined in the IT System Security Plan, "A security incident is any activity that occurs that is a threat to the security of the Institution's information resources. Incidents may be intentional or accidental and jeopardize the availability, integrity or confidentiality of the entity's information and systems. Examples include computer virus attacks, loss of power to the data center, unauthorized access to resources, accidental exposure of sensitive information, etc." NIST 800-61 *Computer Security Incident Handling Guide*, states "Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Continually monitoring for attacks is essential." In FY 2016, Williams Adley found that SI did not have an effective incident detection and response program, due primarily to two factors: (1) lack of continuous monitoring to identify security incidents for response and (2) improper categorization of security incidents based on the most current US-CERT guidance. As a result, the Respond cybersecurity function for SI was defined as Level 1: Ad hoc, in accordance with FY 2016 OIG FISMA maturity metrics.

OCIO is still working to implement an OIG recommendation from the FY 2015 information security audit to automate event monitoring and alerting as part of the ISCM strategy, which had a target date of December 31, 2016. Per the IT Security Program Plan, a key component of

Smithsonian Institution
FY 2016 Information Security Program Review

incident response is continuous monitoring. Without continuous monitoring and automated alerting, it would be extremely challenging for SI personnel to manually identify security event²⁴ patterns because there are thousands of security events each day.²⁵ If a security event is not identified, then it may not get a proper incident response in a timely manner before it has a negative effect on an SI system's confidentiality, integrity, or availability.

Further, while SI did have established procedures for incident response,²⁶ Williams Adley found that SI did not report all incidents to US-CERT²⁷ within the SI-mandated timeframe. Technote IT-930-TN30 IT Security Incident Response Procedures stated that malicious code incidents must be reported within 4 hours of discovery. Of the six incidents reviewed, one, which was a malicious code event, was not submitted in a timely manner.

In addition, as of September 30, 2016, SI used categorizations based on the type of incident (i.e., Category 1: Unauthorized Access, Category 2: Denial of Service), which align with outdated US-CERT requirements; these categorizations do not prioritize an 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, and might escalate to a disaster.

V. Contingency Plans

In FY 2016, SI had not initiated a business impact analysis and was unable to provide an up-to-date disaster recovery plan. As outlined in NIST SP 800-34 *Contingency Planning Guide for Federal Information Systems*, a business impact analysis is the second step in developing a continuity of operations plan and helps to identify key business processes, including the supporting information systems. In turn, the completed business impact analysis dictates the priority of restoration to IT services in the case of a disaster, which is guided by the SI Disaster Recovery Plan. The Disaster Recovery Plan dictates the process that SI must follow to recover from a disaster. However, the SI Technical Standard & Guidelines IT-960-02 Disaster Recovery Planning had not been updated since 2003, although NIST SP 800-34 was revised in 2010.

Without a business impact analysis, OCIO does not have a readily available source for identifying and prioritizing mission-critical systems. Without this detailed prioritization, restoration efforts may not be efficiently or correctly implemented, extending information system downtime. Without up-to-date Disaster Recovery Plan guidance, systems may be unable to recover in a timely manner after a disaster. In the event of an extended outage or disaster, SI

²⁴ A security event is a change in the everyday operations of a network or IT service indicating that a security policy may have been violated or a security safeguard may have failed.

²⁵ *Damballa Q1 2014 Report Shows Average Enterprise Generates 10,000 Security Events Daily*, Damballa.com, May 13, 2014.

²⁶ Office of the Chief Information Officer, SI Technote IT-930-TN30, *IT Security Incident Response Procedures*, Internal Smithsonian Policy, revised January 2015

²⁷ 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.

Smithsonian Institution
FY 2016 Information Security Program Review

must have fully developed and implemented contingency plans that ensure continuity of operations and access to mission-critical business functions.

OCIO managers stated that a business impact analysis was something they would like to complete in the future; however, completing a business impact analysis would require an entity-wide effort driven by the business units and collaboration with OCIO.

VI. Access Control Processes

Effective access control processes are critical in preventing unauthorized dissemination or modification of data because they ensure that only approved and authorized personnel have access to SI information. In FY 2016, SI did not consistently ensure that requests to provide access to a user were properly documented, justified, and authorized prior to granting access. SI also did not have a formalized process for reviewing privileged-user²⁸ access to ensure (1) that access was still required and commensurate with the user's duties and (2) that the user had received required specialized security training before such access was granted.

In FY 2016, Williams Adley found three of 15 sampled privileged users received privileged access before signing the Privileged Rules of Behavior. Of the three, one was a new employee who was granted access in August 2016 and signed the privileged rules of behavior 2 months later in October 2016. In addition, one of 15 sampled administrative users was granted access before completing the privileged-user security training, S-111: Privileged User Security, as required by SI Technote IT-930-TN36. This individual was granted access in August 2016 and completed training in October 2016. SI Technote IT-930-TN36 states that both the elevated rules of behavior and S-111: Privileged User Security training should be completed before privileged access is granted. Technote IT-930-TN36 was effective October 22, 2015, and stipulated that all current privileged users had 90 days to complete the required training and sign the elevated rules of behavior.

In addition, Williams Adley's testing identified 42 SD807 Ex. 2 users with active accounts after 120 days of inactivity. In the FY 2015 IT security program audit, a recommendation was made that OCIO implement an automated process to disable accounts after 90 days of inactivity. As of September 30, 2016, this recommendation remained open, with a target closure date of December 31, 2016.

Without an effective identity and access management practice, there is increased risk of unauthorized system access, by internal employees and by external attackers, endangering the confidentiality, integrity, and availability of SI systems. Also, granting local administrative privilege gives a user the ability to install unapproved and potentially malicious software into the SI network.

VII. Baseline Configurations

Baseline configurations are a set of specifications for a system that have been formally reviewed and agreed on. They are used to ensure that installation of software across the entity is consistent

²⁸ Privileged users have elevated access to different aspects of an entity's network. Access is based on the type of privileged user. Privileged users can install software; modify, delete, or add data and accesses; and perform other activities.

Smithsonian Institution
FY 2016 Information Security Program Review

and secure. Since FY 2014, there has been an open POA&M covering SINet baseline configurations that had not been closed by the end of FY 2016 and had a target closure date of March 31, 2017. This POA&M stated that for several operating systems in use at SI, no baseline configurations existed. Technote IT-960-TN31 required baselines of hardware and software to be identified, documented, and approved and stipulated that deviations from those baselines must also be documented and approved. In FY 2016, Williams Adley determined that no documented approvals existed for the three sampled baseline configuration deviations.

Without documented baseline configurations for software installed in the SI environment, there is a risk that hackers or malicious code can take advantage of inappropriately configured software.

Conclusion

For FY 2016, OCIO had established and taken steps to implement key elements of SI's information security program. However, SI's information security program was not fully effective in reducing information security risks during FY 2016 because of the deficiencies found during this audit and the significant unresolved issues from prior audits. In addition, Williams Adley determined that SI, for the FISMA Detect and Respond processes, was operating at the lowest FISMA metrics maturity level (Level 1: Ad hoc), which is below the Level 4 needed for an effective program.

To strengthen its program, OCIO needs an effective risk-based process to target resources on the highest risk vulnerabilities; establish an enterprise security architecture that aligns security needs with strategic goals; and align disaster recovery plans for information systems based on NIST guidance.

Recommendations

Recommendation 1. Williams Adley recommends that the CIO implement a risk-based approach to prioritizing information security weaknesses identified in the Plan of Action and Milestones (POA&Ms) to ensure the highest risks POA&Ms are resolved first.

Recommendation 2. Williams Adley recommends that the CIO develop and implement an enterprise information security architecture that aligns with SI's strategic plan and mission objectives.

Recommendation 3. Williams Adley recommends that the CIO update SI Technical Standard & Guidelines IT-960-02 Disaster Recovery Planning to reflect current NIST guidance. The CIO also should ensure that current disaster recovery plans and information system contingency plans reflect the changes in guidance.

Smithsonian Institution
FY 2016 Information Security Program Review

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 IT Security Program Plan, October 2014
- h. SI Technote IT-930-TN34, *IT Security System Inventory*, August 2015
- i. SI Technote IT-930-TN29, *IT Security Plans of Actions and Milestones*, June 2015
- j. SI Technote IT-930-TN22, *Security Agreements for Interconnected Systems*, October 2006
- k. SI Technote IT-960-TN31 *Security Configuration Management of Baselines*, September 2012

II. Vulnerability Management

- a. *Smithsonian Institution's IT Security Program Plan*, October 2014
- b. SI Technote IT-930-TN33, *Vulnerability Management Program*, July 2015

III. Enterprise Security Architecture

- a. *Smithsonian Institution's IT Security Program Plan*, October 2014

IV. Incident Response

- a. *Smithsonian Institution's IT Security Program Plan*, October 2014
- b. NIST 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012
- c. SI Technote IT-930-TN30, *IT Security Incident Response Procedures*, January 2015
- d. *US-CERT Federal Incident Notification Guidelines*

V. Contingency Planning

- a. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013
- b. NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010
- c. *Smithsonian Institution's IT Security Program Plan*, October 2014
- d. Technical Standards & Guidelines IT-960-02, *Disaster Recovery Planning*, January 2003

VI. Other Observations for Consideration

Smithsonian Institution
FY 2016 Information Security Program Review

- a. SI Technote IT-930-TN37, *Securing IT Accounts*, October 2015
- b. SI Technote IT-930-TN04, *Disabling & Deleting Dormant User Accounts*, September 2012
- c. SI Technote IT-930-TN36, *Specialized Security Training*, October 2015
- d. SI Technote IT-960-TN31, *Security Configuration Management of Baselines*, May 2016

Smithsonian Institution
FY 2016 Information Security Program Review

Appendix B – Status of Prior Years’ Findings & Recommendations, as of November 20, 2017

Williams Adley did not complete testing on remediation efforts made after September 30, 2016. The recommendations marked as closed after September 30, 2016, will be tested as part of the FY 2017 FISMA audit.

Project Name	Actual Issue Date	Recommendation	Recommendation State	Estimated Implementation Date	Revised Implementation Date	Actual Implementation Date
FY2014 FISMA Audit (A-14-07)	12/14/2015	Strengthen the security assessment and authorization process to align with updated NIST requirements in NIST SP 800-53, Revision 4.	Open	12/31/2016	9/30/2017	
FY2014 FISMA Audit (A-14-07)	12/14/2015	Require system owners to document and maintain a current and accurate listing of all valid exceptions and waivers applicable to the systems we tested (SInet, WebTA, ArtCIS, MGS-STARS, and PANDA).	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Finalize the ISCM strategy in accordance with NIST SP 800-137.	Closed	12/31/2016		1/4/2017
FY2014 FISMA Audit (A-14-07)	12/14/2015	Implement additional controls to ensure the consistent review of POA&Ms for accuracy and completeness.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Update the SInet, webTA, ArtCIS, MGS STARS, and PANDA POA&Ms to include cost estimates.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Implement additional controls to ensure that system sponsors consistently provide to the Director of IT Security quarterly monitoring and reporting on account management activities and audit log reviews.	Closed	12/31/2016		10/7/2016

Smithsonian Institution
FY 2016 Information Security Program Review

FY2014 FISMA Audit (A-14-07)	12/14/2015	Conduct baseline compliance assessments in accordance with the TSG IT-930-02 Security Controls Manual.	Closed	10/31/2016		11/4/2016
FY2014 FISMA Audit (A-14-07)	12/14/2015	Update TN IT-960-TN31 Security Configuration Management of Baselines to be consistent with TSG IT-930-02 Security Controls Manual.	Closed	10/31/2016		11/4/2016
FY2014 FISMA Audit (A-14-07)	12/14/2015	Revise the OCIO Request Form for Network/Email to ensure the form is consistent with the practice for granting access to webTA.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Complete the webTA Security Form for all users with privileged access to the webTA system.	Closed	12/31/2015		12/31/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Implement additional controls to consistently grant access after completion of required training as stated in the PANDA User Access Protocol and retain training documentation to support a user's system privileges.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Assess whether to implement new procedures to disable accounts that have not been logged into for 90 days or accounts that do not have a last-login date in accordance with IT-930-02, Security Control Manual.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Implement additional controls to consistently document MGS STARS access requests to include user name, approval, roles, and user agreements.	Closed	12/14/2015		12/21/2015

Smithsonian Institution
FY 2016 Information Security Program Review

FY2014 FISMA Audit (A-14-07)	12/14/2015	Maintain user agreements and access request forms in a central repository for all users with access to NFC.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Implement technical controls to require multi-factor authentication for all VPN remote access.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Update Smithsonian Directive 920, Life Cycle Management, to require that legacy systems that are no longer supported are retired and replaced.	Closed	12/14/2015		12/21/2015
FY2014 FISMA Audit (A-14-07)	12/14/2015	Develop a list of software versions that are no longer supported by the manufacturer and a plan to upgrade or replace them.	Closed	10/31/2016		10/31/2016
FY 2015 FISMA Audit (A-15-05)	9/30/2016	On a defined frequency, review the current use of local administrator access to ensure access is granted with proper justification and need. In cases where there is a need, split the local administrator privilege into a separate account and remove the privileges for file server/website access. Ensure users with local administrator privilege receive adequate training and understand the responsibilities for having local administrator privilege, such as not using their local administrator access for routine, everyday access and login.	Open	12/31/2017		
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Ensure access requests are properly documented, justified, and authorized prior to granting access.	Closed	8/31/2017		8/31/2017

Smithsonian Institution
FY 2016 Information Security Program Review

FY 2015 FISMA Audit (A-15-05)	9/30/2016	Implement an automated control to disable/remove stale accounts.	Closed	12/31/2016		12/9/2016
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Maintain proper configurations for idle connection time outs and confirm configurations are set properly at least annually.	Closed	3/31/2017		
FY 2015 FISMA Audit (A-15-05)	9/30/2016	We recommend that the system owner develop and implement procedures to manage SOLAA supervisor accounts in accordance with SI's policies.	Closed	3/31/2017		
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Ensure that security events are correlated and alerts are automated if an incident or abnormal activity is detected.	Closed	12/31/2016		3/30/2017
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Provide management oversight to ensure incidents are reported in US-CERT in Si's established timeframes.	Closed	10/31/2016		10/31/2016
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Complete the implementation of the system inventorying process as outlined in the Technical Note IT-930-TN34, IT Security System Inventory.	Open	12/31/2017		
FY 2015 FISMA Audit (A-15-05)	9/30/2016	Develop and implement policies and procedures, including contract terms and conditions, for monitoring security controls performed by cloud system providers.	Closed	1/31/2017		1/4/2017

Smithsonian Institution
FY 2016 Information Security Program Review

FY 2015 FISMA Audit (A-15- 05)	9/30/2016	Review interconnection security agreements to ensure that all documented connections have an agreement in place and that the agreement is current and valid.	Closed	8/31/2017		8/31/2017
FY 2015 FISMA Audit (A-15- 05)	9/30/2016	Fully implement the new IT-930-TN36 Specialized Security Training to ensure personnel with significant security responsibilities complete role-based training and meet specialized IT security training requirements.	Closed	10/31/2016		1/4/2017

Smithsonian Institution
FY 2016 Information Security Program Review

Appendix C – Management’s Response




Smithsonian Institution

Office of the Chief Information Officer

Date: November 2, 2017

To: Cathy L. Helm, Inspector General

From: Deron Burba, Chief Information Officer 

Cc: Al Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
John Benton, Deputy Under Secretary for Finance and Administration
Joan Mockridge, 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
Cindy Zarate, Office of the Chief Financial Officer
Stone Kelly, Office of Planning, Management and Budget

Subject: OCIO Response to “Report on the Smithsonian Institution’s Information Security Program”

Thank you for the opportunity to comment on the report “Report on the Smithsonian Institution’s Information Security Program”.

Management concurs with the recommendations but believes that the findings detailed in the report do not provide a full picture of the status of the Smithsonian’s IT Security Program.

As stated in the report, the Office of the Chief Information Officer (OCIO) developed a plan in late 2014 for enhancing the Smithsonian’s Enterprise IT Security Program to ensure that all critical aspects of computer security are addressed. Each year since then, the Smithsonian has implemented major improvements to the security program in support of the plan. OCIO has made IT security a priority and has accomplished huge strides in advancing the program. There is still more work to reach the program’s goals, but we are well on our way and have a plan to get there.

Examples of security program enhancements that were made in FY16 include:

- Closed 12 findings from previous audits

Chief Information Officer
380 Herndon Parkway
Herndon, VA 20170-4881
MRC 1010
202.633.4901 Telephone
202.312.2804 Fax

Smithsonian Institution
FY 2016 Information Security Program Review

- Developed revised Assessment and Authorization (A&A) process to ensure compliance with NIST 800-53 rev4, including migration to a continuous assessment methodology.
- Acquired and began implementation of a system (RSA Archer) to automate and standardize the A&A, Plan of Actions and Milestones (POA&M), Risk Acceptance (waiver/exception), Privacy Assessment, and other related processes.
- Updated or created several Smithsonian IT security policy and procedure documents
- Implemented role-based specialized security training for all Smithsonian personnel
- Implemented Privacy Awareness training
- Increased security awareness activities including participation in NCSAM and expanding training opportunities
- Developed plan and proposed architecture for integrating and automating the Security, Privacy, PCI Compliance, and Technical Review Board processes.
- Implemented improved vulnerability management program including new scanning tools, standardized scanning processes, vulnerability remediation working groups, and removal of obsolete operating systems.
- Began development of an Enterprise Security Architecture.
- Implemented enhancements to network and perimeter security, including implementation of new web application firewalls, anti-spoofing, enhanced WiFi filtering, proxy SSL interception, and periodic review and optimization of firewall rules.

Additionally, for many of the findings described in the report, remediation was well underway at the time of the audit and was either completed before the issuance of the report or is on target to be completed by the previously agreed due dates.

Please see below for specific responses to each of the report's recommendations.

Please direct any questions you may have regarding the OCIO response to Juliette Sheppard, sheppardj@si.edu, 202-633-5265.

Smithsonian Institution
FY 2016 Information Security Program Review

1. **Williams Adley recommends that the CIO implement a risk-based approach to prioritizing information security weaknesses identified in the Plan of Action and Milestones (POA&Ms) to ensure the highest risks POA&Ms are resolved first.**

OCIO partially concurs with this recommendation. OCIO agrees that at the time of the audit many of the POA&Ms were not up to date or in compliance with requirements. This was partially due to a high amount of staff turnover and partially due to inefficient manual processes. OCIO has now revised its approach to Plans of Actions and Milestones (POA&M) as part of the implementation of the revised A&A process. The revised POA&M process is documented in IT-930-03 and has been automated in the Archer system. The system provides an automated workflow and standardizes required information. The system also facilitates tracking, reporting, and compliance. The revised process includes a risk rating for each POA&M. All new POA&Ms are being created in the automated system and legacy POA&Ms are being migrated to Archer as their systems are migrated into the automated A&A process.

Where feasible, OCIO does address higher risks first. However, due to practicalities, it is not always possible to ensure that the highest risk POA&Ms are resolved first. Often there are dependencies (such as waiting on vendor software updates), operational considerations, or other issues that dictate how quickly an issue can be resolved. Additionally, IT resources are often not interchangeable and you cannot reallocate someone from one system or specialization to another without significant risk. Risk, business/operational considerations, and dependencies all need to be taken into account in planning POA&M resolution.

OCIO will complete the migration of all POA&Ms into the Archer workflow and will further enhance the POA&M process to include justification when the proposed resolution schedule for a high-risk POA&M is affected by dependencies or other considerations.

Expected Completion Date: January 31, 2018

2. **Williams Adley recommends that the CIO develop and implement an enterprise information security architecture that aligns with SI's strategic plan and mission objectives.**

OCIO concurs with this recommendation. OCIO had already begun work on an Enterprise IT Security Architecture before this audit. This includes gathering requirements from a variety of inputs including SI strategic goals, regulatory requirements, industry best practices, identified SI security risks, and operational needs. However, due to higher priorities, completion of this initiative was temporarily deferred. Nonetheless, while work on documenting the comprehensive architecture has been slowed, work has continued on key elements such as defining the ISCM Strategy architecture, enhancing the perimeter security architecture, updating host protection strategies, and implementing additional solutions that fill identified security architecture gaps. Additional architecture gaps have also been documented via the budget planning process. OCIO will resume documentation of the comprehensive architecture once current major projects are completed.

Expected Completion Date: December 31, 2018

Smithsonian Institution
FY 2016 Information Security Program Review

- 3. Williams Adley recommends that the CIO update SI Technical Standard & Guidelines IT-960-02 Disaster Recovery Planning to reflect current NIST guidance. The CIO also should ensure that current disaster recovery plans and information system contingency plans reflect the changes in guidance.**

OCIO concurs with this recommendation. OCIO is the process of planning for a substantial update to its technical strategy for Disaster Recovery, including embracing high availability cloud computing to provide increased coverage and efficiency to system recovery capabilities. OCIO will update disaster recovery policies and procedures to align with this new approach and appropriate best practice guidance. OCIO will then begin working with the units to update their systems' disaster recovery plans and to migrate appropriate systems to the new strategy.

Expected Completion Date: June 30, 2019