Smithsonian Institution

FY 2013 Evaluation of the Smithsonian Institution's Information Security Program

Office of the Inspector General

Report Number A-13-10

July 9, 2014

Smithsonian Institution
Office of the Inspector General

In Brief

FY 2013 Evaluation of the Smithsonian Institution's Information Security Program
Report Number A-13-10, July 9, 2014

Why We Did This Audit

The Federal Information Security Management Act of 2002 (FISMA) directs the Office of the Inspector General to annually evaluate the information security program of the entity. Although not subject to FISMA, the Smithsonian has adopted FISMA through its policy because it is consistent with and advances the Smithsonian's mission and strategic goals.

The objective of this audit was to evaluate the effectiveness of the information security program and practices at the Smithsonian Institution (Smithsonian). We did this by assessing the Smithsonian's compliance with (1) its security policies, standards, and guidelines, and (2) the standards and guidelines promulgated by the National Institute of Standards and Technology (NIST).

Background

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

What We Found

During our fiscal year 2013 audit of the Smithsonian's information security program, we found that OCIO management could strengthen configuration management by timely implementing security patches, improving workstation configuration settings, and deleting obsolete software. In addition, management needs to:

- Strengthen procedures for remote access,
- Improve system backup processes, and
- Ensure that staff are appropriately trained in the areas of incident reporting and security.

Further, we found that Smithsonian Astrophysical Observatory (SAO) management did not fully enforce configuration and account management procedures. We also found that management needed to strengthen its' physical access monitoring capabilities and report on continuous monitoring activities. Lastly, various sections of SAO's system security plan for one system was not current, accurate, or complete.

Finally, we found that the National Museum of Natural History (NMNH) management needed to improve account modification procedures for its research collection information system.

What We Recommended

We made eight recommendations to improve OCIO's information security program. We made five recommendations to SAO and two recommendations to NMNH to improve their information security practices. These recommendations address improvements needed in seven information security control groups: configuration management, access control, physical and environmental protection, contingency planning, incident response, awareness and training, planning, and security assessment and authorization.

Management concurred with our findings and recommendations and has proposed corrective actions.

For additional information, contact the Office of the Inspector General at (202) 633-7050 or visit http://www.si.edu/oig.

Smithsonian Institution Memo

Office of the Inspector General

Date July 9, 2014

To Deron Burba, Chief Information Officer
Danee Gaines Adams, Privacy Officer
Jeanne O'Toole, Director of Office of Protection Services
Juliette Sheppard, Director of Information Technology Security

Cc: Albert Horvath, Under Secretary for Finance and Administration and Chief Financial Officer
Porter N. Wilkinson, Chief of Staff, Board of Regents
Patricia Bartlett, Chief of Staff, Office of the Secretary
Judith Leonard, General Counsel
Cindy Zarate, Executive Officer, Office of the Under Secretary for Finance and Administration/Chief Financial Officer
Stone Kelly, Program and Budget Analyst, Office of Planning, Management and Budget

From Epin Christensen, Acting Inspector General

Subject FY 2013 Evaluation of the Smithsonian Institution's Information Security Program, Report Number A-13-10

Attached please find the final report on our independent evaluation of the Smithsonian's information security program for fiscal year 2013.

We made fifteen recommendations to strengthen the Smithsonian's information security program. Our recommendations addressed the following control groups: configuration management, access control, physical and environmental protection, contingency planning, incident response, awareness and training, planning, and security assessment and authorization.

Management concurred with our findings and recommendations and has proposed corrective actions.

While outside of the scope of this audit, we note that management has filled two key positions, Computer Security Manager and Privacy Officer. We believe that filling these positions is a step to strengthening the information security program at the Smithsonian.

We appreciate the courtesy and cooperation of all Smithsonian staff during this review. Please call me or Joan Mockeridge, Acting Assistant Inspector General for Audits, at 202.633.7050 if you have any questions.

TABLE OF CONTENTS

INTRODUCTION

The goal of information security is to enable an organization to embrace technological innovation while protecting the organization's information and related systems. The objective of this audit was to evaluate the effectiveness of the information security program and practices at the Smithsonian Institution (Smithsonian). We did this by assessing the Smithsonian's compliance with (1) its security policies, standards, and guidelines, and (2) the standards and guidelines promulgated by the National Institute of Standards and Technology (NIST).

This report presents the results of our fiscal year 2013 audit of the information security program implemented by the Smithsonian, based largely on the work of Clifton Larson Allen LLP (CLA), an independent audit, advisory, and public accounting firm.

The E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002, was enacted to strengthen the security controls of federal government information systems. Although the Smithsonian is not subject to the E-Government Act of 2002, the Smithsonian has adopted FISMA through its policy because it is consistent with and advances the Smithsonian's mission and strategic goals.

FISMA requires executive agencies to adopt NIST standards and guidelines as federal information security compliance criteria, which form the basis of many Smithsonian's information security policies and procedures. Furthermore, FISMA requires that the Office of the Inspector General (OIG) perform an annual review of the organization's information security program. FISMA also requires organizations to adopt a risk-based, life-cycle approach to addressing information security that includes annual security program reviews, independent evaluations by the OIG, and reports for the Department of Homeland Security and Congress.

Appendix A contains a detailed outline of our objective, scope, and methodology, and Appendix B contains an update on prior recommendations that have not been fully implemented.

Management concurred with our findings and recommendations and has planned corrective actions to address the recommendations. Refer to Appendix C for management's complete response.

BACKGROUND

This 2013 OIG report of the Smithsonian's information security program included reviews of the following four major systems:

Smithsonian's General Support System (SINet) – SINet is the computing infrastructure and core services used by Smithsonian employees and volunteers to perform their daily work. The services include internet, phone, email, remote access, content filtering, file storage, and many others that are integral to running an organization the size of the Smithsonian.

The research at the Smithsonian Astrophysical Observatory (SAO) focuses on scientific themes such as black holes, dark matter and energy, planets, extreme astrophysics, and the stars. This evaluation included the review of two SAO systems used by the staff of the Harvard-Smithsonian Center for Astrophysics and Scientific Research and their collaborators:

- **Scientific Computing Infrastructure (SCI) System** – The SCI system supports the scientific research mission of SAO and is used to collect, process, store, analyze, and disseminate astrophysical data as well as provide the computing infrastructure to perform theoretical modeling calculations. In addition, SCI consists of all components required to implement scientific computing at SAO including: network and telecommunications infrastructure, servers and storage arrays, scientific workstations and desktops, web servers, and supporting databases.

- **High Energy Astrophysics (HEA) System** – The HEA system supports scientific data reduction/computation, centralized authentication, print, email, data storage, web sites, and database engines. The HEA system also supports the servers that process the telemetry streams from the Chandra telescope operations control center.

National Museum of Natural History (NMNH) - Research Collection Information System (RCIS) – The RCIS system supports the management of over 127 million objects and specimens in diverse fields such as botany, paleobiology, entomology, zoology, mineral sciences, and anthropology. Smithsonian staff, researchers, and staff from the U.S. Geological Survey, and the U.S. Departments of Agriculture, Commerce, and Defense rely on this system.

Smithsonian management identified the SINet, SCI, and HEA systems as moderate impact systems based on Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199 defines system impact as moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. In addition, management identified RCIS as a low impact system, which FIPS 199 defines as having a limited adverse effect on organizational operations, organizational assets, or individuals. The impact level of the system determines which controls management should implement for the particular system.

RESULTS OF AUDIT

This report presents our findings and recommendations for the Office of the Chief Information Officer's (OCIO) information security program and for each major system we reviewed.

I. Configuration Management

Configuration management is an important process for establishing and maintaining secure information system configurations, and provides support for managing security risks in information systems.

<u>OCIO Needs to Improve Configuration Management Practices</u>

We conducted a vulnerability assessment of the SINet infrastructure. We scanned 189 servers, 84 workstations running Windows XP, and 98 workstations running Windows 7, to determine if security patches had been implemented timely. We used the Common Vulnerability Scoring System (CVSS)[1] to determine the risk level of the vulnerabilities. These scans also helped us to verify whether the workstation settings were configured according to the Smithsonian's approved configuration baseline. In addition, we reviewed a sample of router and switch configurations. We identified three areas where Smithsonian could strengthen configuration management by: (1) timely implementing security patches, (2) improving workstation configuration settings, and (3) deleting obsolete software.

[1] A CVSS score is generated using a combination of factors, such as how complex of an attack would be needed to exploit the vulnerability, whether additional information would be needed to exploit the vulnerability, and proximity of the attacker to the target host.

Security Patches

We determined that some security patches were not applied in a timely manner and management did not maintain compliance waivers to document the business justification for not installing the patch. Some unpatched critical and high-risk vulnerabilities were more than 12 months old. The five critical and most of the high-risk vulnerabilities on the servers were in older versions of software. This was also the case with the workstation vulnerabilities.

Smithsonian Technical Notes, IT-960-TN02*, Patch and Update Management of Desktop Computers,* and IT-960-TN33, *Microsoft Server Patching*, provide procedures for evaluating and implementing patches and service packs for Microsoft server and workstation operating systems. For desktops, the process for installing critical patches should begin the day that they are released, and all other patches are generally installed the following month after they are released. For servers running Microsoft operating systems, all patching must occur within 5 business days of the release. These technical notes also assign responsibility for enforcing compliance and maintaining a record of all compliance waivers to the Information Technology (IT) Security Staff.

If critical patches are not applied in a timely manner, the Smithsonian is at an increased risk of attackers exploiting known vulnerabilities in its systems.

Workstation Configuration Settings

We found discrepancies between the configuration applied to the Microsoft Windows workstations and the United States Government Configuration Baseline (USGCB) settings. Our compliance testing tools reported that approximately 10 percent of the 263 USGCB settings were not implemented.

The USGCB settings are promulgated by NIST and are the result of a Federal government-wide initiative to improve and maintain effective configuration settings, focusing primarily on security. NIST recommends that organizations make risk-based decisions as they customize the baseline to support functional requirements in their operational environments and document any changes to the USGCB settings.

The Smithsonian Technical Standards and Guidelines, IT-930-02, *Security Controls Manual* identifies the USGCB settings as the baseline for Microsoft Windows workstations. However, there may be cases where employees, such as scientists and researchers, may need to use a non-compliant configuration setting to run specialized software or equipment. Smithsonian Technical Note IT-960-TN31, *Security Configuration Management of Baselines* allows the OCIO Baseline Manager to request deviations from the baseline configuration if they adequately document the deviation and get approval from the Change Control Board. Although management prepared a report contrasting the differences and accepting the risk between the USGCB settings and the existing configuration settings, they did not identify specific causes or reasons for the deviations.

If management does not document the potential risk and the business reasons for not implementing USGCB configuration settings, they cannot be fully aware of their operational risks.

Obsolete Software

We determined that some network equipment had software versions that were no longer supported by the manufacturer. For example, some switches and routers were running iOS version 12.3, which the manufacturer stopped supporting on March 15, 2012. Many of the server and workstation vulnerabilities we reported above were due to software that was no longer supported by the manufacturer. We also noted that at the time of our audit, the Smithsonian had several hundred workstations running Windows XP, which Microsoft stopped supporting in April 2014.

Because of the risk of continuing to use Windows XP after support ended, OCIO assigned responsibility for replacing workstations running Windows XP to the Periodic Desktop Hardware Replacement Program. Most of those workstations were due to be replaced before Microsoft ended support for Windows XP. Management did not have a similar plan for the routers and switches with obsolete software.

According to NIST special publication 800-40, revision 3, *Guide to Enterprise Patch Management Technologies*, as vendors stop issuing patches to address new security vulnerabilities, the unsupported software becomes less secure and more vulnerable to intrusions than the current versions of the software.

It is necessary to upgrade obsolete products to versions that have ongoing support for patching newly discovered vulnerabilities.

Recommendations

To strengthen configuration management, we recommend that the Chief Information Officer:

1. Ensure that IT security staff enforce compliance with patching requirements and, when appropriate, document compliance waivers.

2. Improve the documentation of USGCB setting deviations to include consideration of risk and the reason for each deviation.

3. Upgrade router and switch software versions that are no longer supported by the manufacturer.

We provided the detailed scanning results to management to assist them in addressing these recommendations.

SAO Needs to Improve Configuration Change Control Procedures

SAO management did not consistently retain change and configuration documentation. In addition, SAO did not consistently request approval from the Change Control Board for configuration changes for the SCI and HEA systems.

SAO IT staff did not consistently follow configuration management procedures when performing necessary system updates. For example, staff did not provide evidence of change requests, approvals, specifications, or test results for any of the six SCI system changes we sampled.

In addition, for a sample of six HEA system changes, staff did not provide evidence of approval for two of them. For the other four, staff did not provide evidence of change requests, approvals, specifications, or test results.

The Smithsonian Technical Standards and Guidelines, IT-930-02, *Security Controls Manual*, Section 3.5.5, *Configuration Change Control (CM-3)*, states that for moderate impact systems, defined as having a serious adverse effect on organizational operations, organizational assets, or individuals if there were to be a loss of confidentiality, integrity, or availability, the IT System Manager or Major System Sponsor must document and control major changes to the information system.

According to Smithsonian Technical Note IT-960-TN01, *Change Management*, the change management process consists of:

- Creating a change ticket;
- Approving the change ticket;
- Notifying customers and IT support staffs of a change when appropriate; and
- Closing the change ticket following implementation.

Also, NIST SP 800-53 Rev. 3 recommends that the organization test, validate, and document configuration management changes.

In the event SAO management does not document, approve, or test configuration changes, those changes could have consequences that adversely affect the system's environment, such as the introduction of new security vulnerabilities or incompatibilities with other system components.

Recommendation

We recommend that the SAO's Computation Facility Department Manager:

4. Enforce configuration management procedures for the SCI and HEA systems to include tracking changes, approvals, testing, and implementation in accordance with Smithsonian policy.

II. Access Control

Access controls limit or detect access to computer resources such as data, programs, equipment, and facilities. These controls help to protect these resources against unauthorized or accidental modification, loss, and disclosure.

OCIO Needs to Strengthen Remote Access Procedures

Management has developed policies for authorizing connections. However, we found that the Smithsonian has not established policies or procedures for detecting and removing unauthorized remote connections. For example, unauthorized connections may include (1) wireless connections to a second network while connected to the Smithsonian network, or (2) an alternative internet service installed by a user to bypass the Smithsonian's firewall or remote access controls.

NIST Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states that an organization should monitor for unauthorized remote connections to the information system, and take appropriate action if an unauthorized connection is discovered.

An unauthorized connection could permit an attacker to circumvent the Smithsonian's access controls and expose the Smithsonian's systems to unauthorized access, data manipulation, and system unavailability.

Recommendation

To ensure that unauthorized remote access is monitored, we recommend that the Chief Information Officer:

5. Develop, document, and implement policies and procedures for detecting and removing unauthorized connections.

SAO Needs to Improve Account Management Procedures for Inactive HEA Accounts

SAO management did not consistently disable or terminate inactive accounts for the HEA system.

For the HEA system, we tested all 416 application accounts and noted that 4 of them were not disabled after 90 days of inactivity or when employment was terminated. These four accounts remained active at the time management generated the accounts report. Three accounts were disabled upon auditor inquiry, and one was already locked. Management determined that the locked account belonged to a separated employee and became locked due to a bad password. Therefore, the account could not be accessed.

The Smithsonian Technical Standards and Guidelines, IT-930-02, *Security Controls Manual*, version 3.8, states that system administrators are responsible for reviewing accounts once every 30 days to identify accounts that have been inactive for 90 days. System administrators should disable accounts that have been inactive for 90 days. The system administrator must take appropriate action to change or delete the accounts of transferred or terminated users and notify that user's unit manager that the account has been disabled and will be deleted after another 90 days unless the manager requests that the account be re-enabled.

In these cases, SAO management did not follow Smithsonian policy for de-activating inactive accounts.

By not disabling inactive accounts or accounts from separated employees, SAO could be subject to unauthorized access, which could lead to data loss, data manipulation, or system unavailability.

Recommendation

We recommend that SAO's Computation Facility Department Manager:

6. Ensure that HEA accounts are reviewed and disabled after 90 days of inactivity or upon personnel/affiliate's departure.

NMNH Needs to Improve Account Modification Procedures

We selected a sample of eight RCIS user accounts. We identified one account that was granted a group permission without approval documented on an Account Modification form. In addition, we identified one user account that belonged to an employee who had transferred positions and no longer required system access.

Smithsonian Technical Standards and Guidelines, IT-930-02, *Security Controls Manual*, version 3.8, states that system administrators are required to review accounts on a monthly basis to identify any transfers or terminations and take appropriate action to change or delete the user's account.

In addition, all changes to RCIS user accounts should be recorded using the Account Modification form. This form is used to document when a user changes permission groups, when an appointment end date is extended, or when an account needs to be deleted.

The addition of a group permission to an RCIS user occurred because NMNH did not document bulk changes to user permissions. For the user who transferred positions, the user's account remained active because the appropriate staff did not review and disable his or her account when access was no longer necessary.

By management not enforcing the use of Account Modification forms, there was an increased risk that users could obtain inappropriate permissions. Inappropriate access may have increased the risk of data loss, data manipulation, and system unavailability.

Recommendations

We recommend that NMNH's Branch Chief for Informatics:

7. Ensure changes to the RCIS user accounts, including modifications of group permissions, are appropriately documented in an Account Modification form.

8. Ensure that RCIS accounts are reviewed and disabled when they are no longer necessary when employees transfer positions.

III. Physical and Environmental Protection

Physical protection (1) limits physical access to information systems, equipment, and the operating environments to authorized individuals only; and (2) protects the facility and support infrastructure housing information systems.

SAO SCI Management Needs to Improve Physical Access Monitoring Capability in the Computer Room

We observed the physical access monitoring capabilities of the SAO SCI computer room, and found that management did not ensure all of the entrances were adequately captured by video cameras. Specifically, we found that the computer room had video surveillance of the front entrance, but there was no camera coverage of the rear and side doors.

NIST Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* states that an organization should monitor physical access to the information system to detect and respond to physical security incidents. Physical access controls require that an organization monitor real-time physical intrusion alarms and surveillance equipment.

Lacking the capability to physically monitor all doors may provide an opportunity for individuals to gain unauthorized access to critical hardware and hinder the investigation of and response to physical security incidents.

Recommendation

We recommend that SAO's Computation Facility Department Manager:

9. Ensure video surveillance coverage of all entrances to the SAO SCI computer room.

During the course of our audit, management installed another video camera to enable the monitoring of all physical access. Therefore, we have closed this recommendation as of the date of this report.

IV. Contingency Planning

Contingency planning establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery. These plans ensure the continuity of operations in emergency situations.

OCIO Needs to Improve Information System Backups

We examined backup processes for the 4 systems we reviewed. However, management did not provide evidence to indicate that backups were performed or that restoration tests were conducted for SINet.

By not adequately ensuring the reliability and integrity of backed-up information, there is a risk that in the event of a disaster, critical information may not be successfully restored.

The Smithsonian Technical Standards and Guidelines, IT-930-02, *Security Controls Manual*, version 3.8, states that all systems must create backups of user-level and system-level information contained in the information system on at least a daily basis. In addition, all systems must employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

Recommendations

We recommend that the Chief Information Officer:

10. Implement corrective action to restore SINet backup processes and capabilities.

11. Periodically perform restoration tests using backup media.

V. Incident Response

Incident response includes adequate preparation, detection, analysis, containment, recovery, and user response activities. Incidents must be tracked, documented, and reported to appropriate organizational officials and/or authorities.

OCIO Needs to Ensure That Staff are Appropriately Trained on Reporting Incidents to US-CERT

We reviewed ten incidents that the Smithsonian was required to report to the United States Computer Emergency Readiness Team (US-CERT). Management did not provide evidence that one of the sampled incidents was reported to US-CERT.

The Smithsonian's Technical Standards and Guidelines, IT-930-TN30, *Incident Response Plan*, version 1.3, assigned responsibility to the OCIO Director for Computer Security or a designated Security Operations Center representative for collecting and reporting data to US-CERT.

We determined that for the one incident not reported, the staff was not properly trained on reporting incidents to the US-CERT as well as what documentation should be retained.

By not reporting all appropriate security incidents, the Smithsonian's and the US-CERT's ability to detect, identify, and respond to suspected or actual breaches of the Smithsonian's computer applications, systems, or network was less effective.

Recommendation

We recommend that the Chief Information Officer:

12. Ensure personnel responsible for reporting incidents to US-CERT have adequate guidance so that all incidents are reported timely.

VI. Awareness and Training

Organizations must ensure that managers and users are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of the organization.

Smithsonian Needs to Ensure that All Personnel Receive Appropriate Security Training

All Smithsonian employees and volunteers with a Smithsonian network account must take the Smithsonian's Computer Security Awareness Training (CSAT). CSAT trains personnel on matters of information systems security, privacy, and physical security, such as granting access to visitors.

In addition, the Smithsonian offers security and privacy awareness training to all employees, including volunteers, when they are credentialed. The employees and volunteers must indicate with their signature that they have received the security and privacy awareness training. However, credentialed volunteers that do not have network accounts do not receive annual security and privacy awareness training because they are only credentialed once every three years.

We reviewed the CSAT records of 26 employees and volunteers who began work during fiscal year 2013. We found that six volunteers had not taken the Smithsonian's CSAT because their job duties did not require network accounts.

The Office of Management and Budget Memorandum (M-12-20) *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* clarifies the intention of FISMA by requiring that all employees receive annual security and privacy awareness training even if they do not access electronic information systems.

The Smithsonian had not yet ensured that credentialed volunteers without network accounts receive annual security training.

Smithsonian personnel without network accounts may not get adequate security training on Smithsonian physical security matters, privacy, and other non-IT issues.

For example, they may not know the policies and procedures for:

- Addressing visitors without Smithsonian badges at restricted areas,
- Handling personally identifiable information, or
- Using personal social media accounts.

Recommendation

We recommend that the Chief Information Officer in coordination with the Office of Protective Services and the Privacy Officer:

13. Provide guidance to employee sponsors of volunteers requiring them to update their volunteers' security awareness training annually.

VII. Planning

The system security plan provides an overview of the security requirements of a system and describes the controls in place or planned for meeting those requirements. The system security plan also identifies responsibilities and expected behavior of all individuals who access the system.

Management Needs to Update the SCI System Security Plan

SAO management did not have an updated SCI System Security Plan (SSP). We reviewed the SSP and determined that it was not current, accurate, or complete for the following sections:

- Firewall Policies
- Modems and Other SINet Remote Access Methods
- Network Router/Switch Installations and Configurations
- Identification and Authentication of Organizational Users
- Device Identification and Authentication
- Baseline Configuration
- Configuration Management Plan
- Information System Backup
- Identification and Authentication of Non-Organizational Users
- Monitoring Physical Access

According to NIST Special Publication 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* an organization should update the SSP to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

SAO management did not update the SSP template for the SCI environment. By not ensuring that the SSP was current, there was a risk that security controls could be incomplete or missing. In addition, staff who rely on the SSP for risk assessment or other purposes may make erroneous decisions based on the information in the plan.

Recommendation

We recommend that SAO's Computation Facility Department Manager:

14. Perform a review of SCI's SSP to ensure that all security control sections are current, accurate, and complete.

During the course of our audit, we verified that SAO management updated their SCI SSP to address the areas that were not current, accurate, or complete. Therefore, we have closed this recommendation as of the date of this report.

VIII. Security Assessment and Authorization

Organizations must periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

SAO HEA Staff Need to Report on Continuous Monitoring Activities

We reviewed OCIO's monitoring logs and noted that HEA staff had not submitted the required quarterly monitoring reports. The Smithsonian Technical Standards and Guidelines IT-930-02, *Security Controls Manual*, version 3.8, specifies quarterly reports and reviews that managers of major systems are required to perform and submit to the OCIO security program.

According to management, HEA staff had not consistently submitted the required reports due to limited program and system resources. HEA staff may not detect system flaws, security vulnerabilities, or system exploitations if they do not perform monitoring activities. If HEA staff do not provide evidence of monitoring activities to OCIO, management will not have the information it requires to determine if the system is being adequately or effectively monitored.

Recommendation

We recommend that SAO's Computation Facility Department Manager:

15. Ensure that SAO HEA staff provide quarterly monitoring reports to OCIO.

During the course of our audit, SAO management began submitting quarterly monitoring reports and audit log reviews to OCIO. Therefore, we have closed this recommendation as of the date of this report.

APPENDIX A

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to evaluate the effectiveness of the Smithsonian's information security program and practices. We did this by assessing the Smithsonian's compliance with (1) its security policies, standards, and guidelines, and (2) the standards and guidelines promulgated by the National Institute of Standards and Technology.

This audit was prepared based on information available as of September 30, 2013. However, we did review data subsequent to September 30, 2013, to close recommendations as of the date of this report.

Clifton Larson Allen audited the Smithsonian's information security program on behalf of the OIG. Their work covered nine of the eleven major control areas in the scope of the audit, with the remaining two performed by OIG auditors.

We provided oversight and review of CLA's work and determined that it was conducted in accordance with Government Auditing Standards, December 2011 Revision, promulgated by the Comptroller General of the United States. Those standards require that the work is planned and performed to obtain sufficient, appropriate evidence that provides a reasonable basis for the findings and conclusions based on the audit objective. We believe that the evidence CLA obtained provides a reasonable basis for our findings and conclusions based on the audit objective.

CLA developed a three-year review rotation plan, in consultation with the OIG, to review the Smithsonian's major systems. CLA reviewed the following four major systems in FY 2013:

1. The Smithsonian's General Support System
2. Smithsonian Astrophysical Observatory - Scientific Computing Infrastructure System
3. Smithsonian Astrophysical Observatory - High Energy Astrophysics System
4. National Museum of Natural History - Research Collection Information System

Our methodology included performing security reviews of the Smithsonian's information technology infrastructure and reviewing the Smithsonian's Plans of Action and Milestones. We performed procedures to test: (a) the implementation of a Smithsonian-wide security program; and (b) operational and technical controls specific to each application such as service continuity, logical access, and change management controls. We also interviewed the Office of the Chief Information Officer staff and major system owners and sponsors.

Generally, all tests were performed to assess the Smithsonian's technical, operational, and management controls over its information security program. For some of the tests performed, we selected samples. Because the samples we selected were not statistical, we cannot project the results of our findings related to these areas across the population.

In addition, we evaluated management's actions to address recommendations from previous FISMA evaluation reports. The results of this evaluation are in Appendix B.

We conducted this performance audit in Washington, DC; Herndon, VA; as well as Boston, MA from October 2013 through March 2014, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

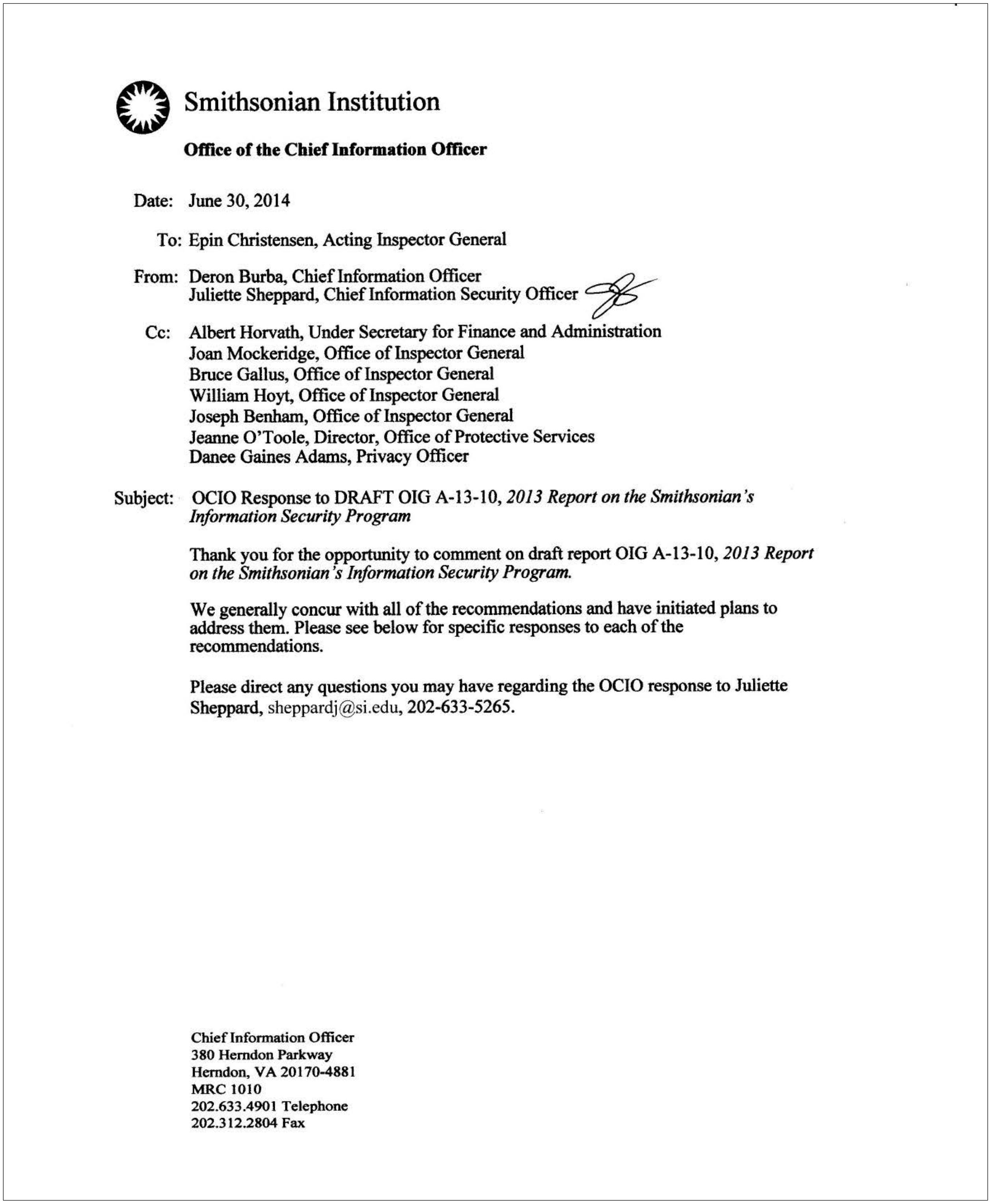
APPENDIX B

Prior Recommendations For Which Corrective Actions Are Not Yet Complete

Report	Recommendation	Current Status
FY 2010 Evaluation of the Smithsonian Institution Information Security Program	Update SD 920 and other related documents to provide clear criteria for designating systems for inclusion in the Institution's FISMA inventory.	Target date for completion 8/30/2014
	Implement controls to ensure that all SI-owned laptops/mobile devices that may be used to store sensitive information are secured with an appropriate encryption technology.	Target date for completion 6/30/2014
Management Advisory Regarding Portable Computer Encryption	Direct Unit IT staff to determine which laptop computers in their inventory may be used to store sensitive data and, with assistance from OCIO, configure those computers with whole drive encryption.	Target date for completion 6/30/2014
	Direct Unit IT staff to identify all laptop computers that will not be configured with encryption and clearly indicate to users with a prominent label that those computers must not be used to store sensitive information.	
	Revise IT-930-TN28 to assign responsibility to staff with the knowledge and skills to ensure laptop computers are configured with appropriate encryption technology.	
FY 2012 Evaluation of the Smithsonian Institution Information Security Program	Work with system managers to more quickly test security patches and updates and remediate all critical and high-risk vulnerabilities identified in the vulnerability assessment that OIG provided to management.	Target date for completion 11/19/2014
	Monitor Smithsonian workstations for the presence of unapproved software and timely maintenance of approved software and enforce the existing policy requiring units to maintain products that are approved.	
	Implement all US Government Configuration Baseline configuration settings for which there is not an approved deviation.	
	Ensure that the system managers provide quarterly monitoring and reporting on account management activities and audit log reviews to the OCIO Security Program.	

APPENDIX C

MANAGEMENT RESPONSE



Smithsonian Institution

Office of the Chief Information Officer

Date: June 30, 2014

To: Epin Christensen, Acting Inspector General

From: Deron Burba, Chief Information Officer
Juliette Sheppard, Chief Information Security Officer

Cc: Albert Horvath, Under Secretary for Finance and Administration
Joan Mockeridge, Office of Inspector General
Bruce Gallus, Office of Inspector General
William Hoyt, Office of Inspector General
Joseph Benham, Office of Inspector General
Jeanne O'Toole, Director, Office of Protective Services
Danee Gaines Adams, Privacy Officer

Subject: OCIO Response to DRAFT OIG A-13-10, *2013 Report on the Smithsonian's Information Security Program*

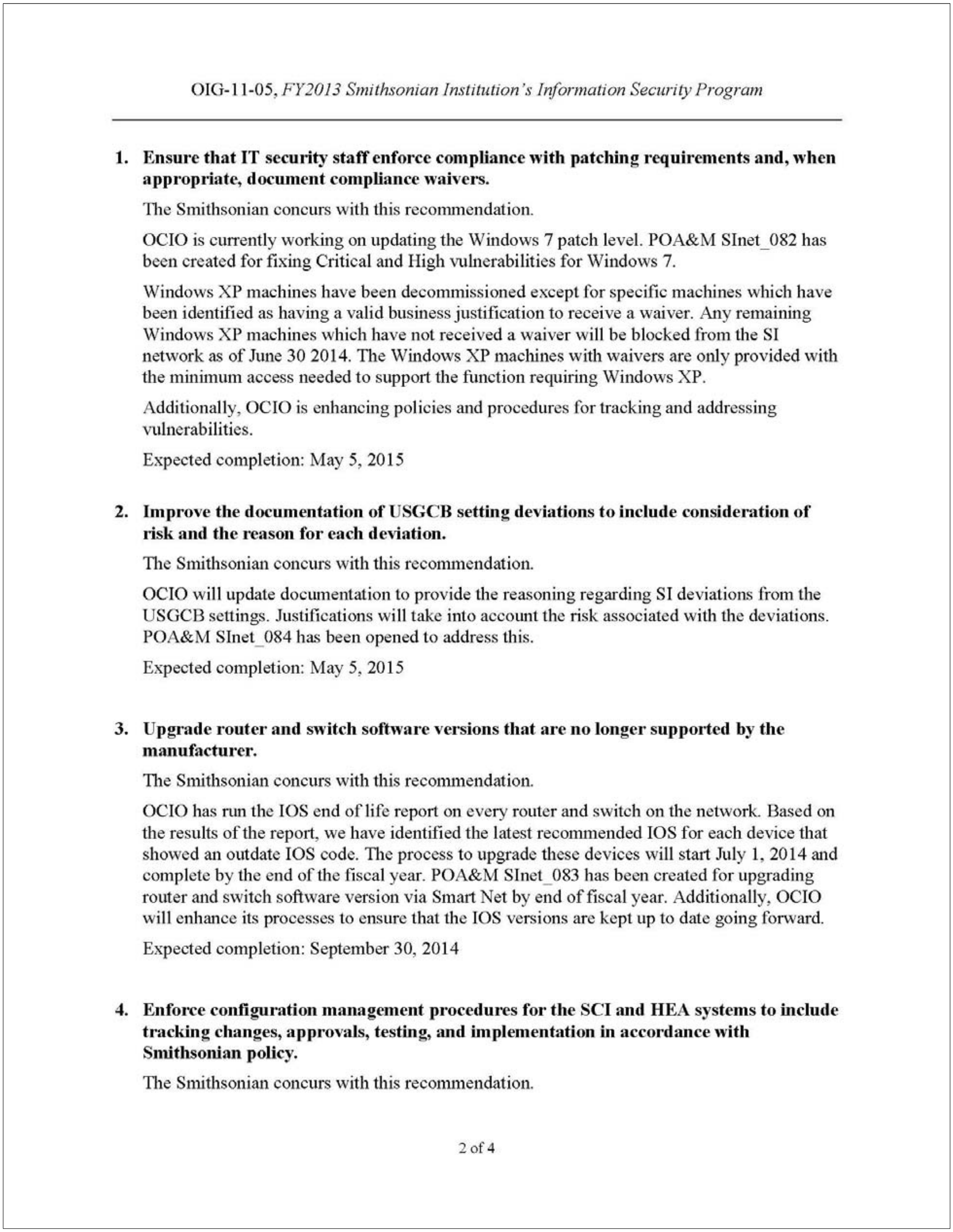
Thank you for the opportunity to comment on draft report OIG A-13-10, *2013 Report on the Smithsonian's Information Security Program.*

We generally concur with all of the recommendations and have initiated plans to address them. Please see below for specific responses to each of the recommendations.

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

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

MANAGEMENT RESPONSE (CONTINUED)



1. **Ensure that IT security staff enforce compliance with patching requirements and, when appropriate, document compliance waivers.**

   The Smithsonian concurs with this recommendation.

   OCIO is currently working on updating the Windows 7 patch level. POA&M SInet_082 has been created for fixing Critical and High vulnerabilities for Windows 7.

   Windows XP machines have been decommissioned except for specific machines which have been identified as having a valid business justification to receive a waiver. Any remaining Windows XP machines which have not received a waiver will be blocked from the SI network as of June 30 2014. The Windows XP machines with waivers are only provided with the minimum access needed to support the function requiring Windows XP.

   Additionally, OCIO is enhancing policies and procedures for tracking and addressing vulnerabilities.

   Expected completion: May 5, 2015

2. **Improve the documentation of USGCB setting deviations to include consideration of risk and the reason for each deviation.**

   The Smithsonian concurs with this recommendation.

   OCIO will update documentation to provide the reasoning regarding SI deviations from the USGCB settings. Justifications will take into account the risk associated with the deviations. POA&M SInet_084 has been opened to address this.

   Expected completion: May 5, 2015

3. **Upgrade router and switch software versions that are no longer supported by the manufacturer.**

   The Smithsonian concurs with this recommendation.

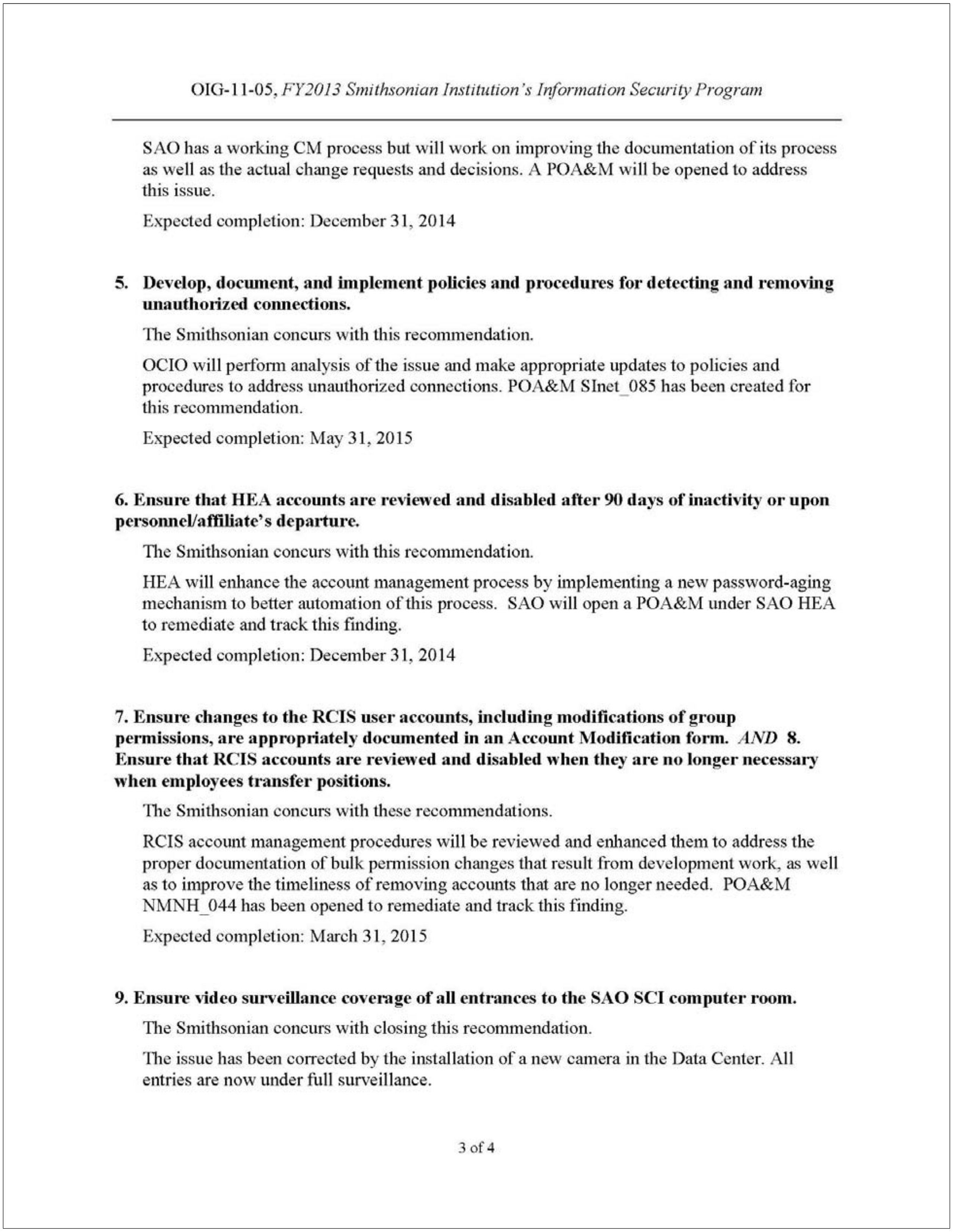
   OCIO has run the IOS end of life report on every router and switch on the network. Based on the results of the report, we have identified the latest recommended IOS for each device that showed an outdate IOS code. The process to upgrade these devices will start July 1, 2014 and complete by the end of the fiscal year. POA&M SInet_083 has been created for upgrading router and switch software version via Smart Net by end of fiscal year. Additionally, OCIO will enhance its processes to ensure that the IOS versions are kept up to date going forward.

   Expected completion: September 30, 2014

4. **Enforce configuration management procedures for the SCI and HEA systems to include tracking changes, approvals, testing, and implementation in accordance with Smithsonian policy.**

   The Smithsonian concurs with this recommendation.

MANAGEMENT RESPONSE (CONTINUED)



SAO has a working CM process but will work on improving the documentation of its process as well as the actual change requests and decisions. A POA&M will be opened to address this issue.

Expected completion: December 31, 2014

5. Develop, document, and implement policies and procedures for detecting and removing unauthorized connections.

The Smithsonian concurs with this recommendation.

OCIO will perform analysis of the issue and make appropriate updates to policies and procedures to address unauthorized connections. POA&M SInet_085 has been created for this recommendation.

Expected completion: May 31, 2015

6. Ensure that HEA accounts are reviewed and disabled after 90 days of inactivity or upon personnel/affiliate's departure.

The Smithsonian concurs with this recommendation.

HEA will enhance the account management process by implementing a new password-aging mechanism to better automation of this process. SAO will open a POA&M under SAO HEA to remediate and track this finding.

Expected completion: December 31, 2014

7. Ensure changes to the RCIS user accounts, including modifications of group permissions, are appropriately documented in an Account Modification form. *AND* **8. Ensure that RCIS accounts are reviewed and disabled when they are no longer necessary when employees transfer positions.**

The Smithsonian concurs with these recommendations.

RCIS account management procedures will be reviewed and enhanced them to address the proper documentation of bulk permission changes that result from development work, as well as to improve the timeliness of removing accounts that are no longer needed. POA&M NMNH_044 has been opened to remediate and track this finding.

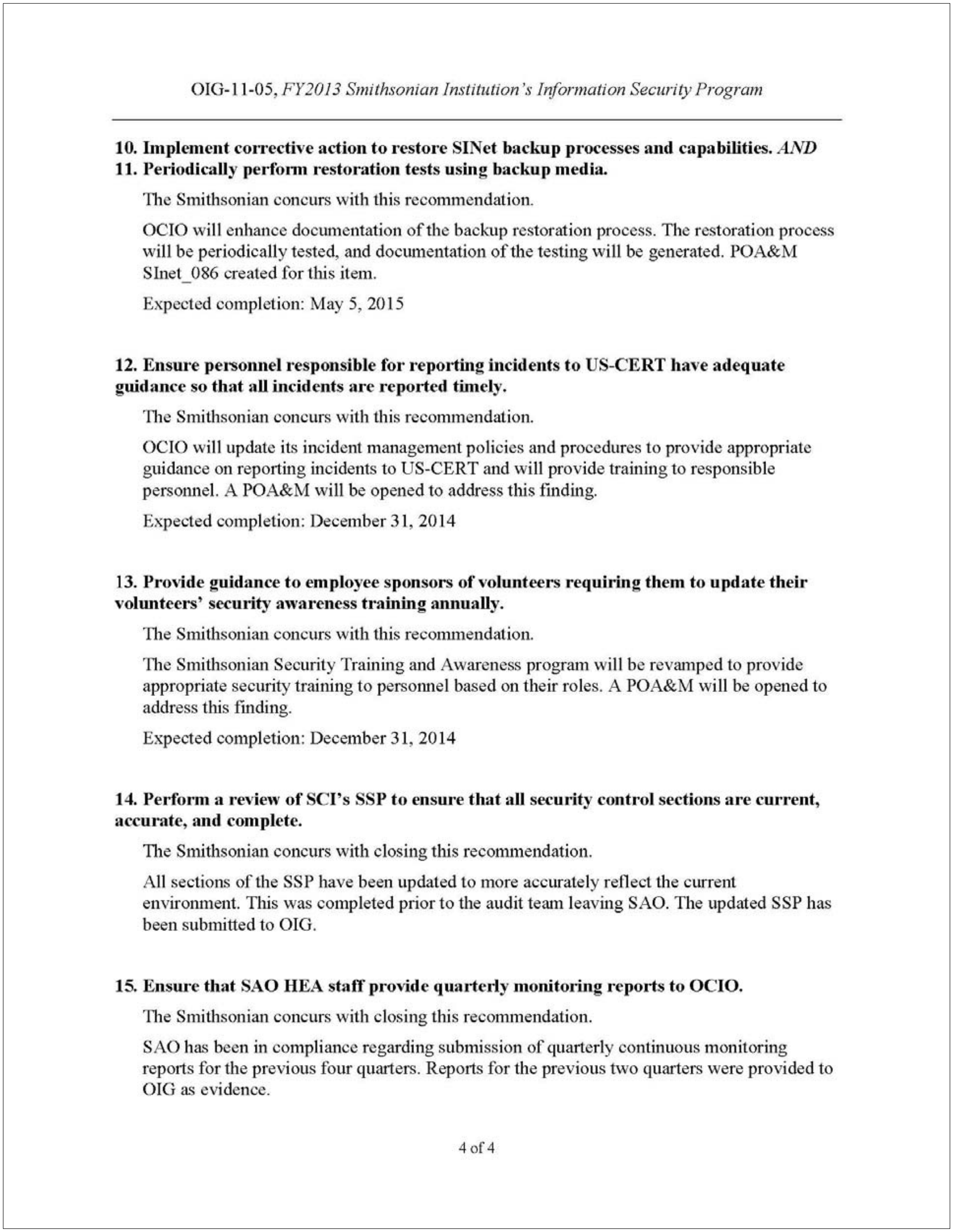
Expected completion: March 31, 2015

9. Ensure video surveillance coverage of all entrances to the SAO SCI computer room.

The Smithsonian concurs with closing this recommendation.

The issue has been corrected by the installation of a new camera in the Data Center. All entries are now under full surveillance.

MANAGEMENT RESPONSE (CONTINUED)



10. Implement corrective action to restore SINet backup processes and capabilities. *AND*
11. Periodically perform restoration tests using backup media.

The Smithsonian concurs with this recommendation.

OCIO will enhance documentation of the backup restoration process. The restoration process will be periodically tested, and documentation of the testing will be generated. POA&M SInet_086 created for this item.

Expected completion: May 5, 2015

12. Ensure personnel responsible for reporting incidents to US-CERT have adequate guidance so that all incidents are reported timely.

The Smithsonian concurs with this recommendation.

OCIO will update its incident management policies and procedures to provide appropriate guidance on reporting incidents to US-CERT and will provide training to responsible personnel. A POA&M will be opened to address this finding.

Expected completion: December 31, 2014

13. Provide guidance to employee sponsors of volunteers requiring them to update their volunteers' security awareness training annually.

The Smithsonian concurs with this recommendation.

The Smithsonian Security Training and Awareness program will be revamped to provide appropriate security training to personnel based on their roles. A POA&M will be opened to address this finding.

Expected completion: December 31, 2014

14. Perform a review of SCI's SSP to ensure that all security control sections are current, accurate, and complete.

The Smithsonian concurs with closing this recommendation.

All sections of the SSP have been updated to more accurately reflect the current environment. This was completed prior to the audit team leaving SAO. The updated SSP has been submitted to OIG.

15. Ensure that SAO HEA staff provide quarterly monitoring reports to OCIO.

The Smithsonian concurs with closing this recommendation.

SAO has been in compliance regarding submission of quarterly continuous monitoring reports for the previous four quarters. Reports for the previous two quarters were provided to OIG as evidence.

APPENDIX D

MAJOR CONTRIBUTORS TO THIS REPORT

Clifton Larson Allen LLP
Bruce Gallus, Supervisory Auditor
William Hoyt, Assistant Inspector General for Operations
Joseph Benham, Auditor