Smithsonian Institution

Memo

Office of the Inspector General

Date June 3, 2013

To Albert Horvath, Under Secretary for Finance & Administration / Chief Financial Officer

Cc G. Wayne Clough, Secretary
Deron Burba, Chief Information Officer
Rebecca Hutchings, Acting Computer Security Manager
Cindy Zarate, Acting Privacy Officer
Stone Kelly, Office of Planning, Management and Budget

From Scott S. Dahl, Inspector General

Subject FY 2012 Evaluation of the Smithsonian's Information Security Program, Report Number A-12-08

Attached please find the final report on our independent evaluation of the Smithsonian's information security program for fiscal year 2012, performed by an independent auditing firm on our behalf. We found four areas where the Smithsonian can make improvements in the information security program. We recommended that management (1) more quickly remediate identified security vulnerabilities and strengthen controls over installed applications; (2) improve workstation configurations; (3) better document deviations from the U.S. Government Configuration Baseline; and (4) improve continuous monitoring and Plan of Actions & Milestones reporting.

The Chief Information Officer concurred with our findings and recommendations and has proposed corrective actions.

While not within the scope of this audit, we note that since January 2013, the Computer Security Manager position has been vacant. We believe that to maintain an effective information security program, this position should be filled expeditiously.

We appreciate the courtesy and cooperation of Smithsonian representatives during this audit. Please contact Michael Sinko or William Hoyt on 202.633.7050 if you have any questions.

Attachment

MRC 524
PO Box 37012
Washington DC 20013-0712
202.633.7050 Telephone
202.633-7079 Fax

Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Information Security Program
Report Number A-12-08, June 3, 2013

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. The Smithsonian voluntarily complies with FISMA requirements because they are consistent with the Smithsonian's strategic goals. We contracted with an independent auditor to conduct this review on our behalf.

Background

The goal of information security is to build a defensible enterprise that enables organizations to harness technological innovation, while protecting an organization's information and information systems.

FISMA requires organizations to adopt a risk-based, life cycle approach to improving information security that includes annual security program reviews, independent evaluations by the Office of the Inspector General, and reporting to the Office of Management and Budget (OMB) and the Congress. FISMA, DHS and the National Institute of Standards and Technology (NIST) also identify security requirements for federal information security programs.

What We Found

We determined that during the past year, the Office of the Chief Information Officer (OCIO) made improvements in the Smithsonian's information security program, including proactively reviewing security controls and identifying areas to enhance the program. While the Smithsonian has made progress, it needs to continue to make improvements to ensure controls are in place and operating effectively.

We found weaknesses in the following areas:

The Smithsonian needs to make the following two improvements to the information security program --

- More timely test and install security patches and updates
- Strengthen desktop workstation configuration baselines

At the system level, managers of four major applications need to improve continuous monitoring or Plan of Actions and Milestones (POA&M) reporting.

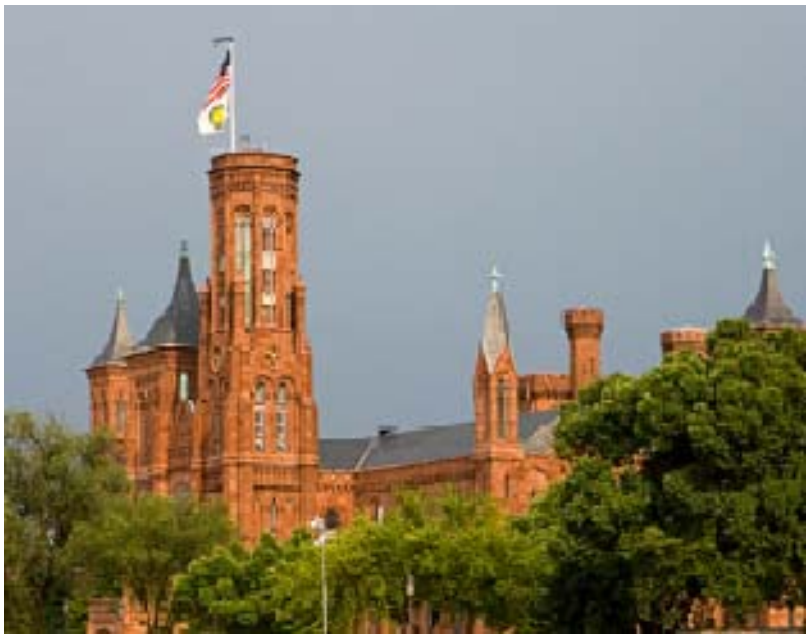
We also noted that OCIO has not completed implementing 11 information security recommendations from previous reports. By not implementing these recommendations, the Smithsonian's IT infrastructure and systems may be more vulnerable to unauthorized modifications and access, as well as the unavailability of important resources.

What We Recommended

We made six recommendations to more quickly remediate identified security vulnerabilities; strengthen controls over installed applications; improve workstation configurations; better document deviations from established baselines; and improve continuous monitoring and POA&M reporting.

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

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

2012 INDEPENDENT EVALUATION REPORT

CliftonLarsonAllen

REPORT ON FISCAL YEAR 2012
Independent Evaluation of the Smithsonian Institution's
Information Security Program

TABLE OF CONTENTS

REPORT ON FISCAL YEAR 2012
Independent Evaluation of the Smithsonian Institution's
Information Security Program

On behalf of the Office of the Inspector General (OIG), the auditing firm of CliftonLarsonAllen (CLA) conducted an independent audit of the Smithsonian's information security management program and practices consistent with Title III of the 2002 E-Government Act, also known as the Federal Information Security Management Act (FISMA).

We found that the Smithsonian made considerable progress in improving controls over information technology resources. However, the Smithsonian needs to do additional work to ensure controls are in place and operating effectively. We noted some control weaknesses relating to the Office of the Chief Information Officer (OCIO) not implementing security patches or software updates in a timely manner and not configuring Smithsonian workstations in accordance with the US Government Configuration Baseline (USGCB). We also found that system managers were not consistently submitting quarterly monitoring reports or remediating security vulnerabilities within established timeframes.

PURPOSE

FISMA was enacted to strengthen the security of federal government information systems. Although the Smithsonian is not subject to FISMA because it is not an executive agency, the Smithsonian has adopted FISMA through its Technical Standards and Guidelines (TSG).

FISMA outlines federal information security compliance criteria, including the requirement for an annual independent assessment by the OIG. This report presents the results of the Smithsonian's OIG annual evaluation of the information security controls implemented by the Smithsonian, based on the work performed by CLA.

BACKGROUND

The goal of information security is to build a defensible enterprise that enables organizations to harness technological innovation, while protecting an organization's information and information systems.

FISMA requires organizations to adopt a risk-based, life-cycle approach to improving information security that includes annual security program reviews, independent evaluations by the OIG, and reporting to the Department of Homeland Security (DHS) and the Congress. FISMA, DHS, and the National Institute of Standards and Technology (NIST) also identify security requirements for federal information security programs. These include:

- Security assessments conducted as part of an information system security authorization or re-authorization process; and

- Continuous monitoring activities, including testing and evaluating the information systems as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

REPORT ON FISCAL YEAR 2012
Independent Evaluation of the Smithsonian Institution's
Information Security Program

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this evaluation were to assess the effectiveness of the Smithsonian's information security program and practices and to determine compliance with FISMA requirements and the Smithsonian's security policies, procedures, standards, and guidelines.

On behalf of the OIG, the audit firm CLA performed an independent performance audit of the Smithsonian's information security management program. We conducted this audit in accordance with *Government Auditing Standards*, December 2011 Revision, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides 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 objectives.

Our methodology included performing security reviews of the Smithsonian's information technology (IT) infrastructure and reviewing the Smithsonian's Plans of Action and Milestones (POA&Ms). We also based our audit on detailed interviews with the OCIO personnel and major system owners or sponsors. CLA developed a three year audit rotation plan, in consultation with the OIG, to review the Smithsonian's 17 major systems. We evaluated the following subset of seven major systems in FY 2012, which includes one contractor operated system:

- Enterprise Resource Planning Financial (ERP Financial)
- Smithsonian Tracking and Applicant Referral System (MGS STARS)
- OFEO OPS Security Management System
- General Support System (SI Net)
- Natural Museum of American Indian – Collection Information System
- Smithsonian Institution Research Information System
- Natural Museum of American History – Collection Information System (NMAH CIS Multi MIMSY)

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. Additionally, we evaluated management's actions to address recommendations from previous FISMA evaluation reports.

We performed our review from October 1, 2012, through November 15, 2012, at the Smithsonian's facilities in Washington, DC and Virginia. The Smithsonian's management and staff were helpful and accommodating throughout this review. This evaluation was prepared based on information available as of October 31, 2012.

REPORT ON FISCAL YEAR 2012
Independent Evaluation of the Smithsonian Institution's
Information Security Program

SUMMARY OF RESULTS

Improvements from Last Year

Our audit of the Smithsonian's security management program and practices determined that during the past year, OCIO made marked improvements to strengthen their information security program, including proactively reviewing security controls and identifying areas to enhance the program. As part of its ongoing security program, the Smithsonian periodically performed network scanning, updated its information security policies and procedures to reflect its current operating environment, performed risk assessments of minor applications, designed and implemented Interconnection Security Agreements with all external systems interfacing with Smithsonian systems, monitored all 17 major applications for compliance with Smithsonian policies and federal regulations, and re-certified and re-accredited major systems consistent with NIST guidance.

Current Year Findings

We found control weaknesses in FY 2012 relating to the Smithsonian not implementing security patches or software updates in a timely manner and not configuring Smithsonian workstations in accordance with the USGCB. We also found that system managers did not consistently remediate security vulnerabilities within established timeframes or report progress to the Computer Security Manager. As a result, Smithsonian information systems have known security vulnerabilities that, if exploited, could result in unauthorized access, data loss, or a reduction in systems availability. In addition, two system managers did not consistently submit quarterly monitoring reports to the Computer Security Manager. Consequently, the Smithsonian could not ensure that these system managers were adequately monitoring the security posture of systems under their custody.

Moreover, the Smithsonian needs to make greater progress implementing recommendations from prior reports. The Status of Prior-Year Findings and Recommendations table at the end of this report details the status of each of the 11 IT security and 6 privacy open recommendations. One of these recommendations is over four years old. By not implementing these recommendations, the Smithsonian's information technology (IT) infrastructure may be more vulnerable to unauthorized modifications and access, as well as the unavailability of important resources. The following are some of the more important IT security recommendations from prior reports:

- Develop, document, and implement controls to ensure Smithsonian policy is updated timely to include new IT requirements and disseminated to system sponsors and contractors.
- Centrally document as part of its on-going risk management process the decisions by the Under Secretaries and the Unit managers to include or exclude systems in the FISMA inventory.
- Implement controls to ensure that all Smithsonian-owned laptops/mobile devices that may be used to store sensitive information are secured with an appropriate encryption technology.
- Ensure that continuous monitoring of major systems is operating effectively, and that the major system points of contact (POCs) provide reports on quarterly monitoring and reporting to the OCIO Security Program on account management activities and audit log reviews.
- Improve the current server and standard desktop workstation procedures to identify any required operating system (OS) or application security patches.

The following is the most important privacy recommendation from prior reports:

- Develop, document, and implement privacy policies and procedures to support an overall privacy program that adequately addresses privacy-related risks. Without comprehensive privacy policies and procedures in place, the Smithsonian is at greater risk for inappropriately handling or disclosing sensitive personally-identifiable information (PII). In addition, the lack of clear privacy policies or procedures for describing and defining sensitive PII, and how sensitive PII should be handled, greatly increases the likelihood that individuals who come into contact with sensitive PII will handle it inappropriately.

The following is a more detailed discussion of the control weaknesses we found in our current evaluation, as well as recommendations for strengthening the Smithsonian's information security program. We present our findings in the order of greatest risk to the Smithsonian.

Management concurred with our findings and recommendations and has proposed corrective actions that will address the recommendations. Please refer to Appendix A for management's complete response.

DETAILS OF RESULTS

I. More Timely Test and Install Security Patches and Updates

We assessed 250 servers and over 850 infrastructure components. We also conducted a vulnerability assessment of 181 desktop computers of the Smithsonian's approximately 4,300 desktop computers. We determined that the Smithsonian did not consistently implement security patches and software updates on Smithsonian computers in a timely manner.

Of the 250 servers, we found that nearly 20% had un-patched vulnerabilities that are considered critical or high-risk according to the Common Vulnerability Scoring System (CVSS), version 2. 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. Critical and high-risk vulnerabilities can be exploited by a person with little skill and are considered certain, or likely, to have an adverse impact on confidentiality, integrity, or availability of the systems.

According to management, many of these vulnerabilities exist on servers for which the system manager does not have adequate resources to test the patches and updates. As a result, the system managers are wary of implementing those patches and updates in the production environment.

In addition, we determined that some servers and desktop computers were using outdated software that may no longer be supported by the vendor, or for which security updates may no longer be developed. Examples of outdated and vulnerable software include Oracle Java versions from December 2008, Adobe products from 2010, and missing Microsoft patches and updates from as early as 2009. The Smithsonian was not consistently or timely installing security patches or updates for software that was part of the Smithsonian's standard desktop and server software installations. This is a repeat finding from last year, the target date has been revised and the completion date was set for May 2013.

We also found software on workstations that is not part of the Smithsonian's standard configuration, such as Firefox, iTunes, Safari, and RealPlayer, that was not patched or updated in a timely manner. This software was missing patches more than six months old. According to management, they made improvements to their monitoring processes that detect these issues but need to improve the timeliness of acting on that information.

SI Technical Note IT-960-TN02, *Patch and Update Management of Desktop Computers* states that it "establishes the procedures for evaluating and implementing patches and service packs from Microsoft and updates from Apple for desktop computers. Timely implementation of vendor fixes is critical to ensuring that Smithsonian desktop computers remain secure and function optimally." The system administrator will schedule the application of the patch with the Change Control Board and adhere to the standard user notification requirements outlined in the Technical Note.

SI Technical Note IT-960-TN33, *Microsoft Server Patching,* establishes the procedures for evaluating and implementing Microsoft critical patches, non-critical patches, and service packs to Microsoft server operating systems in use at the Smithsonian. According to this technical note, "a *critical patch* is one that needs to be immediately deployed to all Smithsonian Servers because of a specific threat to system resources."

Smithsonian Directive 940, *Acquisition of Information Technology Products*, states that units must obtain approval from OCIO before acquiring IT products that are not part of the Smithsonian's technical reference model and thus not part of the standard inventory. The directive further states that "units that receive permission to acquire non-preferred IT products are responsible for maintaining the product; for example, addressing any cyber-security flaws that may be announced…."

System administrators of Windows, UNIX and other operating systems are required to apply security patches in a timely manner. One of the most frequent reasons hackers can gain access to a computer system is un-patched software.

The conditions noted above result in servers and desktop computers being unprotected against actively exploited vulnerabilities. These vulnerabilities expose the Smithsonian's computer assets, operating systems, applications and data to unauthorized access, data loss, data manipulation, and a reduction of system availability. Once a patch is released, the risk increases for unpatched systems. Hackers can analyze the patch to determine the nature of a security flaw and how to exploit it on the unpatched system.

Recommendations:

The Chief Information Officer (CIO) should expedite the implementation of existing recommendations to improve the patch management process and test and implement updates for the Smithsonian's standard desktop and server software.

In addition, we recommend that the CIO:

1. 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.

2. 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.

II. Strengthen Desktop Workstation Configuration Baselines

The USGCB is the baseline configuration for the Microsoft Windows XP and Windows 7 operating systems promulgated by NIST. Our tests for USGCB compliance found a significant percentage of configuration settings failures on Smithsonian desktop computers. Eleven of the 181 machines tested for USGCB compliance presented failure rates over 70%. The Smithsonian has provided documentation that management formally accepted the risks resulting from the deviations from the USGCB settings, but did not include technical or business reasons to support these deviations as required by Smithsonian policy.

IT-960-TN31, *Security Configuration Management of Baselines,* states: "The Smithsonian uses NIST-recommended benchmarks and compliance tools."

TSG IT-930-02, *Security Controls Manual*, Section 3.5.6 Configuration Settings (CM-6), states: "Where systems do not comply with the baseline configuration, all deviations must be fully documented with both technical and business reasons that the control was not implemented."

The deviations from the baseline may result in desktop computers being insufficiently protected against vulnerabilities. These vulnerabilities may expose the Smithsonian's computer assets, operating systems, applications, and data to unauthorized access, data loss, data manipulation, and a reduction of system availability. If the deviations are properly documented, management may choose to accept them or may determine that the Smithsonian is exposed to greater risk than it is willing to accept.

Recommendations:

We recommend that the CIO:

3. Improve the documentation of accepted deviations from the US Government Configuration Baseline by clearly indicating the mission or business justification for accepting the residual risk. The waiver should be reviewed as part of the SINet authorization to operate at least every 3 years.
4. Implement all US Government Configuration Baseline configuration settings for which there is not an approved deviation.

III. System Managers Need to Improve Continuous Monitoring Reporting

The Systems Managers for SINet and the NMAH CIS Multi MIMSY system did not consistently provide quarterly monitoring reports to the OCIO. As a result, OCIO could not ensure that these system managers were monitoring the security posture of systems under their custody, as required by Smithsonian policy and FISMA guidance. We note that SINet is the general support system and is a moderate-impact system.

The two system managers were not systematically following TSG IT-930-02 Appendix D on Continuous Monitoring & Compliance Reports. The SINet System Manager did not provide Audit and Security Logs for the 1st and 2nd quarters of FY12. Also, the NMAH CIS Multi MIMSY system manager did not provide Audit and Security log reviews for the 4th quarter of FY12. At the program level, the OCIO maintains a monitoring scorecard that includes POA&M and compliance reporting and noted these failures. Management cited a high level of turnover in key management positions during the last 18 months as the reason for the system managers not consistently meeting reporting requirements. Some of the affected positions included system sponsors who are responsible for supervising the system managers.

TSG IT-930-02 *Security Controls Manual*, version 3.8, dated September 2012, states:

> *3.4.7 Continuous Monitoring (CA-7)*
> Continuous monitoring activities include configuration management and controls of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The Smithsonian has established as a baseline a minimum selection of items for control monitoring. Each automated information system or Unit may also select additional subsets of the security controls for purposes of continuous monitoring. Reports that are required for baseline monitoring are found in Appendix D.

Recommendation:

5. We recommend that the system sponsors for SINet and NMAH CIS Multi MIMSY ensure that the system managers provide quarterly monitoring and reporting on account management activities and audit log reviews to the OCIO Security Program.

IV. System Managers Need to Improve POA&M Reporting

A Plan of Actions and Milestones (POA&M) is created and tracked when the OIG or OCIO identifies a deficiency that requires correction. The POA&M identifies tasks needing to be accomplished, the resources required to accomplish the tasks, significant milestones, and scheduled completion dates for the milestones. We reviewed the POA&Ms of systems selected for testing this fiscal year to determine if milestone remediation dates were established and adhered to. We found instances where POA&M remediation dates were not being met for improvements to the ERP Financial and the MGS STARS systems. Management cited a high level of turnover in key management positions during the last 18 months as the reason for delays in POA&M implementation and reporting.

TSG IT-930-02 Security Controls Manual, version 3.8, dated September 2012, states:

> *3.4.5 Plan of Action and Milestones (CA-5)*
> An information system POA&M documents the Unit's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
>
> The Unit's Major System Sponsor is expected to track POA&Ms. The IT System's staff is expected to action and update POA&Ms on a continuing basis. All system and program POA&Ms must be

reviewed and updated no less than quarterly, and any changes on POA&M status reported to the OCIO.

Un-remediated security vulnerabilities may expose Smithsonian systems to a loss of confidentiality, integrity, or availability.

Recommendation:

6. The system sponsors for ERP Financial and MGS STARS systems should ensure that system managers timely implement and update POA&Ms and report changes of status to the OCIO security program.

REPORT ON FISCAL YEAR 2012
Independent Evaluation of the Smithsonian Institution's
Information Security Program

Status of prior years' findings and recommendations

The following table presents the open recommendations from prior reports:

Report	Finding	Recommendation	Current Status
SAO Scientific Computing Infrastructure Audit #A-08-03 Issued Sept. 30, 2008	Controls were not adequate to ensure that the Smithsonian Astrophysical Observatory (SAO) SSP was reviewed and updated in accordance with OMB and NIST policy.	The OCIO should develop, document, and implement controls to ensure Smithsonian policy is updated timely to include new IT requirements and disseminated to system sponsors and contractors.	Target date revised to June 2013.
FISMA Evaluation Report Audit #A-10-01 Issued March 15, 2011	The method used for determining the FISMA Systems inventory was not based on a risk analysis.	Update Smithsonian Directive (SD) 920 and other related documents to provide clear criteria for designating systems for inclusion in the Smithsonian's FISMA inventory.	Target date revised to April 2013.
	The method used for determining the FISMA Systems inventory was not based on a risk analysis.	Centrally document as part of its on-going risk management process the decisions by the Undersecretaries and the Unit managers to include or exclude systems in the FISMA inventory.	Target date March 2013.
	The Smithsonian did not effectively enforce the SI policy stated in IT-930-TN28 that requires all mobile devices used to store sensitive data to be encrypted.	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 revised to December 2013.
FISMA Evaluation Report Audit #A-11-05 Issued May 15, 2012	Management controls were not operating effectively to ensure all of the major system points of contact were providing periodic monitoring and POA&M reports to OCIO and that reasonable remediation dates were being met for resolving and/or correcting security weaknesses.	Ensure that continuous monitoring of major systems is operating effectively, and that the major system POCs, provide reports on quarterly monitoring and reporting to the OCIO Security Program on account management activities and audit log reviews.	Target date December 2013.
	Management controls were not operating effectively to ensure all of the major system points of contact were providing periodic monitoring and POA&M reports to OCIO and that reasonable remediation dates were being met for resolving and/or correcting security weaknesses.	Ensure the major system POCs provide quarterly POA&M progress updates to the OCIO Security Program, and notify the CIO and Unit Directors when the system or program POA&M scheduled completion dates are not being met.	Target date December 2013.
	Controls were not operating effectively to ensure that security patches were implemented on Smithsonian computers in a timely manner.	Improve the current server and standard desktop workstation procedures to identify any required OS or application security patches.	Target date February 2014.
	Controls were not operating effectively to ensure that security patches were implemented on Smithsonian	Test and provide patch updates for the Smithsonian's standard desktop workstation software inventory within 30 days for vendor	Target date May 2013.

Report	Finding	Recommendation	Current Status
	computers in a timely manner.	identified critical security patches and 60 days for vendor identified high risk security patches following the release of the patch.	
Management Advisory Regarding Portable Computer Encryption Advisory #M-13-01 Issued March 4, 2013	The Smithsonian did not effectively enforce the SI policy stated in IT-930-TN28 that requires all mobile devices used to store sensitive data to be encrypted.	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 December 2013
	The Smithsonian did not effectively enforce the SI policy stated in IT-930-TN28 that requires all mobile devices used to store sensitive data to be encrypted.	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.	Target date December 2013
	The Smithsonian did not effectively enforce the SI policy stated in IT-930-TN28 that requires all mobile devices used to store sensitive data to be encrypted.	Revise IT-930-TN28 to assign responsibility to staff with the knowledge and skills to ensure laptop computers are configured with appropriate encryption technology.	Target date May 2013
FY 2008 Privacy Program Evaluation Audit #A-08-08 Issued May 29, 2009	The Smithsonian had not developed, documented, or Implemented Privacy Policies and Procedures.	The Senior Agency Official for Privacy should develop, document, and implement privacy policies and procedures to support an overall privacy program that adequately addresses privacy-related risks.	Target date revised to April 2013.
	The Smithsonian had not identified or documented the types or locations of sensitive personally identifiable information.	Establish and implement requirements to reduce holdings of PII to the extent practicable.	Target date revised to April 2013.
	The Smithsonian's privacy impact assessment process needed improvement.	Develop, document, and implement procedures for conducting PIAs. Procedures for completing PIAs should address relevant Smithsonian requirements.	Target date revised to April 2013.
	The Smithsonian's privacy impact assessment process needed improvement.	Post completed privacy impact assessments on the Smithsonian's public website.	Target date revised to April 2013.
	Physical controls at the Smithsonian were not adequate to protect sensitive personally identifiable information.	Develop, document, and implement policies and procedures for safeguarding documents containing PII.	Target date revised to April 2013.
	Physical controls at the Smithsonian were not adequate to protect sensitive personally identifiable information.	Develop and implement procedures to enforce compliance with new and existing privacy policies related to the protection of sensitive documents containing PII.	Target date revised to April 2013.

MANAGEMENT'S RESPONSE **Appendix A**

Smithsonian Institution

Office of the Chief Information Officer

Date: May 23, 2013

To: Scott S. Dahl
Inspector General

From: Deron Burba, Chief Information Officer

cc: Albert Horvath, Under Secretary for Finance and Administration / Chief Financial Officer
Michael Sinko, Assistant Inspector General for Audits
William Hoyt, OIG Unit IT Director, Administrative Officer
Bruce Gallus, OIG Supervisory Auditor
Rebecca Hutchings, Acting Director Computer Security, OCIO
Martin D. Beckman, Director, IT Operations, OCIO
Jeffrey McAvoy, Manager Data CTR OPS & Network Server Admin, OCIO
Joseph Johnston, Manager Network Management Division OCIO
Randy Bender, Manager Customer Support Services Division, OCIO
Karen Garlick, Assistant Director Collections Management Services, NMAH
Rick Luhrs, Chief Technology Officer, NMAH
Raelene Worthington, MIMSY XG Manager, NMAH
Huyen Tran, Director Office of System Modernization, OCIO
Curtis Lutz, Director HR & Admin Systems Division, OCIO
Stone Kelly, Office of Planning Management and Budget
auditrecommendation@oig.si.edu

Subject: OCIO Response to OIG A-12-08, *FISMA 2012 Independent Evaluation Report*

Thank you for the opportunity to comment on your draft report on the *Independent Evaluation of the Smithsonian Institution's Information Security Program.*

In response to the annual review, the attachment provides a summary of proposed OCIO actions. If the OIG does not believe the projected evidence will be sufficient for closure, please let us know so we can adjust our plan.

Please direct any questions you may have regarding the OCIO response to Rebecca Hutchings, HutchingsR@si.edu 202-633-0632.

Attachment

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

The Smithsonian Institution is not subject to the E-Government Act of 2002 / Title III and the OMB guidelines implementing that Act and is also not subject to the E-Government Act Section 208 guidance as it relates to the Privacy Act of 1974. To the extent that Federal Information Security Management Act (FISMA) and OMB guidance reflect best practices, are reasonable in the context of the Smithsonian, and are not in conflict with the Institution's own statutory obligations (the increase and diffusion of knowledge), it is the Institution's practice to secure its information consistent with the available resources and provisions of the Act and OMB guidance.

OIG Recommendation #1

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.

Concur. The OCIO Network Management Division (NMD) is working to improve patch management support and timeliness for all the major FISMA systems core/critical servers particularly for SOLARIS and LINUX operating system baselines. **Scheduled completion date is 19 November 2014.**

OIG Recommendation #2

We recommend that the CIO 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.

Concur. The OCIO Customer Support Services Division (CCSD) Desktop support team continues to work to improve SI's desktop software monitoring reviews. Standard Software dashboards continue to be published quarterly. Units are expected to continue to request non-standard desktop software waivers from the OCIO System Architecture and Product Assurance (SAPA) staff using Technology Waiver Requests. While maintenance of non-standard software remains a responsibility of the product requestor, the OCIO is working to improve tracking of critical or high desktop software vulnerabilities and to notify Units when remediation is expected. The OCIO Data Center Operations & Network Server Administration Division (DCO&NSAD) is also working with the CCSD and OCIO Help Desk staff to ensure SI's standard desktops automatically received policy and desktop software updates. **Scheduled Completion Date is 19 November 2014.**

OIG Recommendation #3

We recommend the CIO improve the documentation of accepted deviations from the US Government Configuration Baseline (USGCB) by clearly indicating the mission or business justification for accepting the residual risk. The waiver should be reviewed as part of the SInet authorization to operate at least every 3 years.

Concur. The OCIO DCO&NSAD will continue to document the USGCB settings and identify the mission or business justifications for any deviations. Starting in FY13, the documented justifications will be included as part of the SInet security risk management review with the mission and system sponsor. **Scheduled completion date is 20 November 2013.**

OIG Recommendation #4

We recommend the CIO implement all US Government Configuration Baseline configuration settings for which there is not an approved deviation.

Concur. The OCIO CCSD and DCO&NSAD will work to ensure the OCIO implements the SI approved desktop baseline configuration settings. An annual report will be provided to help track compliance efforts. **Scheduled completion date is 19 November 2014.**

OIG Recommendation #5

We recommend that the system sponsors for SInet and NMAH CIS Multi MIMSY ensure that the System managers provide quarterly monitoring and reporting on account management activities and audit log reviews to the OCIO Security Program.

Concur. For SInet's core/critical servers, as identified in the SInet assessment boundary, the SInet ISSO has been requested to improve monthly monitoring and quarterly OCIO program reporting particularly for assurances that audit log are being reviewed. For NMAH CIS Multi MIMSY, the OCIO OSM staff has been requested to improve monthly audit log reviews and quarterly reporting and the NMAH CIS Staff has been requested to improve monthly user account management reviews and quarterly OCIO program reporting. **Scheduled completion date is 19 November 2014.**

OIG Recommendation #6

The system sponsors for ERP Financial and MGS STARS systems should ensure that System Managers timely implement and update POA&Ms and report changes of status to the OCIO security program.

Concur. For the ERP Financial and MGS Stars systems, the OCIO ERP ISSO has been requested to improve POA&M updates and reviews. Evidence of improved FY13 quarterly status reports will be provided to the OIG as evidence for requesting closure. **Scheduled completion date is 30 October 2013.**