Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Information Security Program
Report Number A-11-05, May 15, 2012

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 it is consistent with its strategic goals. We hired 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, OMB 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 to strengthen the 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 performs network and system scans and annually provides security assessments and/or authorizations for all major systems, consistent with NIST guidance.

However, additional work is still needed to ensure controls are in place and operating effectively. We found weaknesses in four areas where OCIO did not do the following:

- Maintain evidence that software changes were tested and approved before the changes were implemented;
- Provide timely updates to its Technical Security Notes, hence the units did not always adhere to the employee separation process concerning the disabling or termination of user accounts;
- Enforce the requirement that units submit quarterly monitoring reports; and
- Implement security patches in a timely manner.

We also noted that OCIO has not completed addressing 12 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 nine recommendations to strengthen configuration change controls; improve user account management; enforce requirements for continuous monitoring reports; and strengthen patch management and flaw remediation.

Management concurred with our findings and recommendations and has proposed corrective actions that, if timely implemented, will resolve the recommendations.

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)

2011 INDEPENDENT EVALUATION REPORT

CliftonLarsonAllen

This page intentionally left blank

REPORT ON FISCAL YEAR 2011
Independent Evaluation of the Smithsonian Institution's
Information Security Program

TABLE OF CONTENTS

This page intentionally left blank

REPORT ON FISCAL YEAR 2011
Independent Evaluation of the Smithsonian Institution's Information Security Program

On behalf of the Office of the Inspector General (OIG), CliftonLarsonAllen (CLA) conducted an independent evaluation 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).

PURPOSE

The E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA), was enacted to strengthen the security of federal government information systems.

The Smithsonian is not subject to the E-Government Act of 2002, nor is subject to the OMB guidelines implementing the Act and the E-Government Act Section 208 guidance as it relates to the Privacy Act of 1974. However, it is the Smithsonian's practice to secure its information consistent with the available resources and provisions of the two statutes as well as OMB guidelines.

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

The privacy provisions of the E-Government Act require federal organizations to ensure sufficient protections for the privacy of personal information as federal organizations implement citizen-centered electronic Government. Federal organizations are directed to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when federal organizations develop or buy new IT systems to handle collections of personally identifiable information. Federal organizations are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

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. To maximize the timeliness and integrity of security-related information, the collection of data should be a by-product of existing continuous monitoring processes.

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 Office of Management and Budget and the Congress. FISMA, OMB 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, to include testing and evaluating the information

system 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).

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, CliftonLarsonAllen LLP performed an independent evaluation of the Smithsonian's information security management program. We conducted this evaluation in accordance with *Government Auditing Standards*, July 2007 Revision, as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform an 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 objectives.

We followed a work plan based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*; NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;* NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems*; NIST Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems;* and our general controls review methodology.

Our procedures included performing security reviews of the Smithsonian's information technology (IT) infrastructure and major systems, and reviewing the Smithsonian's Plans of Action and Milestones (POA&Ms). We also based our audit on detailed interviews with the Office of the Chief Information Officer's (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 seventeen major systems. We evaluated the following subset of six major systems in FY 2011, which includes one contractor operated system:

- Web Time & Attendance (WebTA)
- Smithsonian Tracking and Applicant Referral System (MGS STARS)
- OFEO Facilities Management System (FMS)
- Smithsonian Network (SINet)— the Smithsonian's general support system
- Smithsonian Online Academic Appointment System (SOLAA)
- Art Collection Information System (ARTCIS)

We performed these procedures to test (1) the implementation of a Smithsonian-wide security program, and (2) operational and technical controls specific to each system such as service continuity, logical access, and change controls. Additionally, we evaluated management's actions completed through September 30, 2011, to address prior years' recommendations.

We also evaluated the Smithsonian's privacy program, interviewed the Senior Privacy Officer (SPO) and reviewed prior years' privacy program recommendations.

We performed our review from October 7, 2011, through November 18, 2011, at Smithsonian's Office of the Inspector General in Washington, D.C. the Office of the Chief Information Officer at the Smithsonian data center.

Smithsonian's management and staff were helpful and accommodating throughout this review and assisted us in refining the recommendations. This independent evaluation was prepared based on information available as of October 31, 2011.

DETAIL OF RESULTS

Our audit of the Smithsonian's security management program and practices determined that during the past year, OCIO made improvements to strengthen the 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 performs network and system scans and annually provides security assessments and/or authorizations for all major systems, consistent with NIST's guidance.

However, additional work is still needed to ensure controls are in place and operating effectively. We found weaknesses in FY 2011 in the following four areas where OCIO did not do the following:

- Maintain evidence that software changes were tested and approved before the changes were implemented;
- Provide timely updates to its Technical Security Notes, hence the units did not always adhere to the employee separation process concerning the disabling or termination of user accounts;
- Enforce the requirement that units submit quarterly monitoring reports; and
- Implement security patches in a timely manner.

Management concurred with our findings and recommendations and has proposed corrective actions that will resolve the recommendations. Management's full response is attached to this report.

We also noted that 17 prior years' information security recommendations were closed in FY 2011 and 12 prior years' information security recommendations directed to OCIO remain open, including four recommendations from the FY 2010 FISMA report. The following is a list of some of the more important open recommendations from prior year reports:

- Re-assess the security categorization for major systems currently categorized as low-impact systems, based on the type of PII stored in the system. The systems should either be re-classified as moderate or the security categorization revised to include adequate justification for classifying the system as low.
- Ensure that all major and minor systems are addressed in system security plans in accordance with OMB and NIST guidelines. OCIO should ensure controls over major

and minor systems are identified, documented, and implemented based on their impact on the Smithsonian or sensitivity of data they process or store.

- Establish procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced.

- 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.

We also noted that one privacy program recommendation was closed in FY 2011, and 8 prior year privacy program related recommendations remain open from the FY 2008 Privacy Program Evaluation report. This FY 2008 report recommended that the Smithsonian 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 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 Smithsonian needs to make greater progress in implementing important information security and privacy recommendations from prior reports.

The Status of Prior-Years' Findings and Recommendations table, included in this report, documents the details for 20 open recommendations. One recommendation is as many as five years old. 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.

The Smithsonian continues to make progress on implementing recommendations from previous reports, including:

- Updating all major systems security plans and clarifying security assessment boundaries.

- After field work for this audit was completed, OCIO documented, justified, and formally accepted deviations from the Federal Desktop Core Configuration (FDCC) settings.

The following is a more detailed discussion of the four new control weaknesses identified above that we found in our FY 2011 FISMA evaluation, as well as recommendations for strengthening management controls over the Smithsonian's information security program. We present our findings in the order of greatest risk to the Smithsonian.

I. Configuration Change Control Needs to be Strengthened

Controls were not operating effectively to ensure that software changes were tested and approved before being migrated into the production environment. The Change Control Board (CCB) did not maintain documentation for the testing/approval of software changes.

The CCB did not have evidence for changes selected for review, including software upgrades, firewall changes, and server replacements. Missing documentation included the following:

- None of the eight tickets tested had any evidence that testing was approved; and

- Management has not developed a process to consistently document evidence of testing of changes.

Information systems are typically in a constant state of change as organizations add new capabilities, correct software flaws, address security threats, and for other valid reasons. To ensure that these necessary changes do not introduce new vulnerabilities or adversely affect the operation of the system, NIST recommends that organizations adopt a well-defined configuration management process that includes testing and approval of the changes.

Specifically, NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations, CM-3,* provides the following characteristics of a well-defined change control process:

(1) The organization:
   a) Determines the types of changes to the information system that were configuration controlled;
   b) Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;
   c) Documents approved configuration-controlled changes to the system;
   d) Retains and reviews records of configuration-controlled changes to the system;
   e) Audits activities associated with configuration-controlled changes to the system; and
   f) Coordinates and provides oversight for configuration change control activities through the Change Control Board that convenes [*frequency*] [*organization-defined configuration change conditions*].

(2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

The Smithsonian defined its configuration change control process in its Technical Standards and Guidelines as follows:

> *Moderate and High Impact systems must meet the following requirements:*
> The Unit's IT System Manager or Major System Sponsor must document and control major changes to the Unit's major information system. The Technical Review Board must approve significant changes, and the Change Control Board should be requested to approve all changes in which the production system will be taken off-line. The Unit's IT System Manager or Major System Sponsor may approve minor changes.
>
> Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. The Unit's IT System Manager or Major System Sponsor must include emergency changes in the configuration change control process.[1]

[1] SI Technical Standards and Guidelines (TSG) IT-930-02 *Security Controls Manual*, Section 3.5.3 Configuration Change Control (CM-3)

The lack of evidence that OCIO is ensuring changes are tested as part of the change control process could increase risks to system availability and integrity. OCIO's CCB needs to ensure adequate documentation of changes and approvals to the Smithsonian systems in order to prevent any unauthorized or inappropriate modification of the operating environment.

Recommendation:

1. We recommend that the Chief Information Officer (CIO) establish and implement additional Change Control Board (CCB) procedures, which more clearly document the types of changes that are required to undergo testing prior to being moved into the production environment, or that the CCB would accept any residual risk.

II. User Account Management Needs Improvement

Controls were not operating effectively to ensure that access to the Smithsonian's information technology resources was adequately controlled. Specifically, the process for documenting the termination of access for employees and contractors was not properly followed and/or enforced. We noted that the documentation for termination of access (i.e. the HEAT[2] ticket) was not available for eight out of twenty-four separated employees and contractors. No evidence was available to determine whether access was disabled or terminated promptly upon notification.

TSG IT-930-02 "Security Control Manual" required that inactive accounts be disabled after 90 days. The Security Program Procedures IT-930-TN04, "*Disabling and Deleting Dormant Accounts,*" was out-of-date and was not in compliance with the overarching SI Security Policy. TN04 indicated that inactive accounts will be disabled after 30 days and needs to be updated to be consistent with the Security Control Manual. According to the CIO, after we completed our fieldwork, OCIO published an update for IT-930-TN04 and began the process of updating IT-930-02 to address this issue.

The appropriate organization officials for the Art Collection Information System (ARTCIS)[3] and the Smithsonian Online Academic Appointment System (SOLAA)[4] were not submitting the proper access request forms. Hence*,* System Sponsors did not consistently enforce the access request process across all units.

According to OCIO management, limited personnel resources have hindered timely updates to the Smithsonian's Technical Notes on security. The Smithsonian's employee separation process was not always adhered to by appropriate organization officials. In addition, ARTCIS

[2] HEAT is a commercial helpdesk issue management software suite.

[3] ARTCIS is based on *The Museum System (TMS)* and serves the internal collections management needs of ten of the Smithsonian's museums. ARTCIS provides the public with easy access to more than 600,000 works of art.

[4] SOLAA is an automated system for processing internships, fellowships and other academic appointments. The mission of the SOLAA system is to provide one common portal and process to accept academic appointment applications from the public and provide management of the applications by each unit.

and SOLAA System Sponsors need to implement the Smithsonian's formal access request procedures.

User account management procedures are implemented to ensure that only authorized users have access to an organization's resources. When an employee or contractor leaves an organization or no longer has a need to access an organization's resources, their access privileges should be revoked. The Smithsonian's Technical Standards and Guidelines assign responsibility for user account management to system administrators. System administrators are responsible for:

- reviewing accounts once every 30 days to identify accounts that have been inactive for 90 days;
- disabling accounts that have been inactive for 90 days;
- notifying their unit manager that the account has been disabled;
- deleting after another 90 days (for a total of 180 days of inactivity). [5]

Technical Note, IT-960-TN-12, "*Active Directory Account and Password Requests,"* dated September 18, 2007, states: In order to adhere to the procedures in this technical note, all IT support staff that provision and maintain Active Directory accounts must use OCIO's supported HEAT system.

Terminated employees or contractors may retain access and transferred employees may have access to resources to which they are not entitled. Inadequate user account management procedures exposes the Smithsonian's IT resources to potential unauthorized access, data loss, and data manipulation.

In his response to this report, the CIO stated that OCIO has implemented improvements in the exit clearance process to ensure separated employee and contractor access to the Smithsonian network is terminated according to existing policies.

Recommendations:

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

2. Ensure that Technical Note, IT-930-TN04, *Disabling and Deleting Dormant Accounts*" aligns with TSG IT-930-02, *Security Controls Manual.*

3. Enforce the termination process for employees and contractors leaving the Smithsonian and ensure that the OCIO Help Desk removes separated employees and contractors' access to SINet in accordance with Smithsonian policies and procedures.

We recommend that the Systems Sponsor for ARTCIS:

4. Develop and implement formal access request procedures to ensure that access is properly documented and approved to adequately enforce the principle of "least privilege".

[5] IT-930-02, *Security Controls Manual*, version 3.5, *Dormant Accounts.*

We recommend that the Systems Sponsor for SOLAA:

5. Develop and implement formal access request procedures to ensure that access is properly documented and approved to adequately enforce the principle of "least privilege".

III. Smithsonian Units Are not Consistently Submitting Quarterly Monitoring and POA&M Reports

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.

According to NIST, organizations demonstrate adequate due diligence by continuously monitoring security controls to ensure that they continue to be effective in light of changes to information systems and their operating environment that inevitably occur. OCIO has a monitoring process that tracks POA&Ms and compliance reporting.[6] Several information systems' Points of Contact did not consistently provide evidence of quarterly monitoring reports[7] to OCIO. Also, we noted several instances where POA&M remediation dates were delayed.

According to OCIO, limited system resources have delayed the correction and resolution of POA&Ms.

The Smithsonian has defined continuous monitoring activities in its Technical Standards and Guidelines*:*

> 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 AIS 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.[8]

The Smithsonian has assigned responsibility for implementing POA&Ms to correct weaknesses in its IT systems in the following technical note:

> The Unit Director is responsible for ensuring that an individual is assigned to manage applicable program POA&Ms for their unit and that the assigned person is responsible for ensuring planned tasks are completed.

[6] NIST Special Publication 800-37, Appendix G.

[7] The quarterly reports are specified in Technical Notes TN02 and TN04.

[8] SI Technical Standards and Guidelines (TSG) IT-930-02 *Security Controls Manual*, version 3.5, dated February 2011, section *3.4.7 Continuous Monitoring (CA-7)*.

> The Unit IT Director or the OIG-designated recipient of the original report is responsible for identifying evidence to justify closure of the program audit recommendation.[9]

Preparing continuous monitoring reports helps to ensure that system sponsors effectively manage their systems. POA&M reports help management to ensure that weaknesses in IT systems are addressed in a timely manner. Without these reports, OCIO cannot ensure that system sponsors are following the Smithsonian policies and managing their systems effectively.

Recommendations:

To enforce the OCIO's requirements for quarterly reporting, we recommend that the CIO:

6. 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.

7. 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.

IV. Patch Management / Flaw Remediation Controls need to be Strengthened for Servers and Desktop Workstations

Controls were not operating effectively to ensure that security patches were implemented on Smithsonian computers (Servers and desktop workstations) in a timely manner.

From a targeted sample of 110 desktop workstations, we successfully tested 71 terminals to determine the version of the installed software. Some of these workstations were using outdated software that may no longer be supported by the vendor, or for which security updates may no longer be available. Approximately 70% of the targets tested were using Java versions from December 2008; 18% were missing Adobe product updates from 2010; 8% were missing Microsoft patches from 2009, 2010 and 2011 and approximately 60% of the target computers were missing QuickTime patches.

Therefore, software that was part of the installed OCIO desktop standard software inventory on the Smithsonian's computer systems was not consistently being patched for security issues on a timely basis.

In addition, there was several 3rd party products (Firefox, iTunes, Safari, and RealPlayer) which appear on less than 10% of the tested sample, that were missing patches more than 6 months old.

One of the most frequent reasons hackers are able to gain access to systems is when they are not patched with security updates. The Smithsonian has established patch management policies and procedures through its Technical Standards and Guidelines and Technical Notes.

[9] SI Technical Note, IT-930-TN29, *IT Security Plans of Actions and Milestones*

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." This technical note further states that "Timely implementation of vendor fixes is critical to ensuring that the Smithsonian computers, servers and desktop workstations remain secure and function optimally."

SI Technical Standards and Guidelines, IT-930-02, *Security Controls Manual*, 3.17.2 Flaw Remediation (SI-2), states that:

> IT-960-TN02, *Patch and Service Pack Implementation for Desktop PCs* outlines requirements for applying patches. 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.
>
> IT-930-TN08, *Implementing Vendor Software Patches/Fixes* details the procedures on implementing vendor software patches and fixes on desktop systems.
>
> NIST has a vulnerability database available at http://nvd.nist.gov where it is possible to check on known software product vulnerabilities.

Moderate and High Impact systems must meet the following requirements:

> The organization employs automated systems to determine the status of flaw remediation.

The conditions noted above can result in server and desktop workstations 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.

Recommendations:

To strengthen patch management and flaw remediation controls, we recommend that the CIO:

8. Improve the current server and standard desktop workstation procedures to identify any required operating system (OS) or application security patches.

9. Test and provide patch updates for the Smithsonian's standard desktop workstation software inventory within 30 days for vendor identified critical security patches and 60 days for vendor identified high risk security patches following the release of the patch.

STATUS OF PRIOR YEARS FINDINGS AND RECOMMENDATIONS

The following table represents the current status of the prior years' information security system and program recommendations, 12 recommendations remain open and 17 recommendations were closed in FY 2011:

Report	Date Issued	Recommendation	Current Status
FY 2006 FISMA Reviews			
The Smithsonian Institution's Information Security Program A-06-05	4/20/2007	Establish procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced.	Target date revised to 9/15/2012
Smithsonian Institution Network (SINet) Audit A-06-07	8/10/2007	Enforce separation of duty controls noted in the SINet system security plan and specifically segregate system administration roles from security roles.	**Closed**
FY 2007 FISMA Reviews			
Human Resources Management System A-07-06	9/19/2007	Identify, document, and implement segregation of duty controls for sensitive administrative and system support functions. Management should document in the system security plan those activities that need to be segregated.	**Closed**
		Enforce Institution policy and procedures requiring the weekly review of logs and monthly submission of appropriately detailed management reports to OCIO.	**Closed**
		Document final baselines for the HRMS operating system and database after determining what Institution-wide baselines will be adopted and specifically note where suggested security settings have not been implemented for valid business purposes.	**Closed**
ID and Badging, C-CURE Central, and Central Monitoring Systems A-07-07	3/31/2008	Implement baselines for the various components of the system including all databases and operating systems. In addition, where suggested security settings cannot be implemented for valid business purposes, management should document their deviations from the baseline.	**Closed**
The Smithsonian Institution's Information Security Program A-07-08	3/31/2008	Ensure that all major and minor systems are addressed in system security plans in accordance with OMB and NIST guidelines. OCIO should ensure controls over major and minor systems are identified, documented, and implemented based on their impact on the Smithsonian or sensitivity of data they process or store.	Target date revised to 9/15/2012

Report	Date Issued	Recommendation	Current Status
FY 2008 FISMA Reviews			
Smithsonian Astrophysical Observatory Scientific Computing Infrastructure A-08-03	9/30/2008	OCIO needs to 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 7/15/2012
		Ensure system sponsors implement NIST, OMB, and Smithsonian requirements within required timeframes.	**Closed**
		Logically segregate public-facing SAO Web sites from internal areas by transferring or migrating these sites inside a DMZ.	**Closed**
		Comply with IT-960-TN16 and maintain individual server configuration documents for each server by system owner. In addition, fully document all instances where suggested security configurations are not followed, due to technical limitations or valid business reasons, and this documentation should reflect management acceptance of associated risks.	**Closed**
		Comply with Smithsonian policy and enforce a 15-minute lock on all Solaris and Linux machines after exceeding the prescribed number of consecutive invalid access attempts.	**Closed**
		Implement session lock controls for Linux- and Solaris-based machines that automatically activate after no more than 20 minutes of inactivity.	**Closed**
		Research tools that will enable automatic review of account activity for Solaris NIS. If such tools cannot be identified, management should document this deficiency in the risk assessment and system security plan. In addition, if automated controls cannot be implemented, identify compensating controls that will reduce risks associated with not having automated account management controls.	**Closed**
		Adhere to Smithsonian policies and provide security awareness training to all staff within 30 days of hire.	**Closed**
NMNH EMu Application A-08-04	10/7/2008	Ensure that all individuals who have direct access to Institution information system resources, including those without SINet accounts, sign the required rules of behavior forms and complete security awareness training.	**Closed**

Report	Date Issued	Recommendation	Current Status
		Enforce Institution policy and procedures requiring submission of appropriately detailed management reports to OCIO based on the frequency described within Appendix E of Technical Standards & Guidelines IT-930-02, IT Security Controls Manual, either monthly, quarterly or annually, depending on the reportable item.	**Closed**
The Smithsonian Institution's Information Security Program A-08-09	3/17/2009	Ensure that general security awareness training is available and enforce the requirement that all employees, contractors, volunteers, visiting scholars, and interns complete the training.	**Closed**
		Ensure the implementation of FDCC requirements across all domains at the Smithsonian and document any deviations.	**Closed**
		Identify all of the Smithsonian's public websites that use e-authentication.	Target date revised to 9/15/2012
		Complete risk assessments for each public website that uses e-authentication, in accordance with OMB guidance.	Target date revised to 9/15/2012
		Approve an Institution-wide initiative to develop, design, and implement a mechanism to track and monitor all employees, contractors, volunteers, visiting scholars, and interns, for compliance with general security awareness training, regardless of access to an Institution computer or network.	**Closed**
FY 2009 FISMA Reviews			
Fiscal Year 2009 Independent FISMA Audit Of The Smithsonian Institution's Information Security Program A-09-11	6/30/2010	Re-assess the security categorization for major systems currently categorized as low-impact systems, based on the type of PII stored in the system. The systems should either be re-classified as moderate or the security categorization revised to include adequate justification for classifying the system as low.	Target date 10/15/2012
		To further strengthen the interconnections process, ensure that all interconnections have signed agreements prior to execution.	Target date 9/30/2012
FY 2010 FISMA Reviews			
FISMA Evaluation Report A-10-01	3/15/2011	Update SD 920 and other related documents to provide clear criteria for designating systems for inclusion in the Smithsonian's FISMA inventory.	Target date 9/15/2012

REPORT ON FISCAL YEAR 2011
Independent Evaluation of the Smithsonian Institution's
Information Security Program

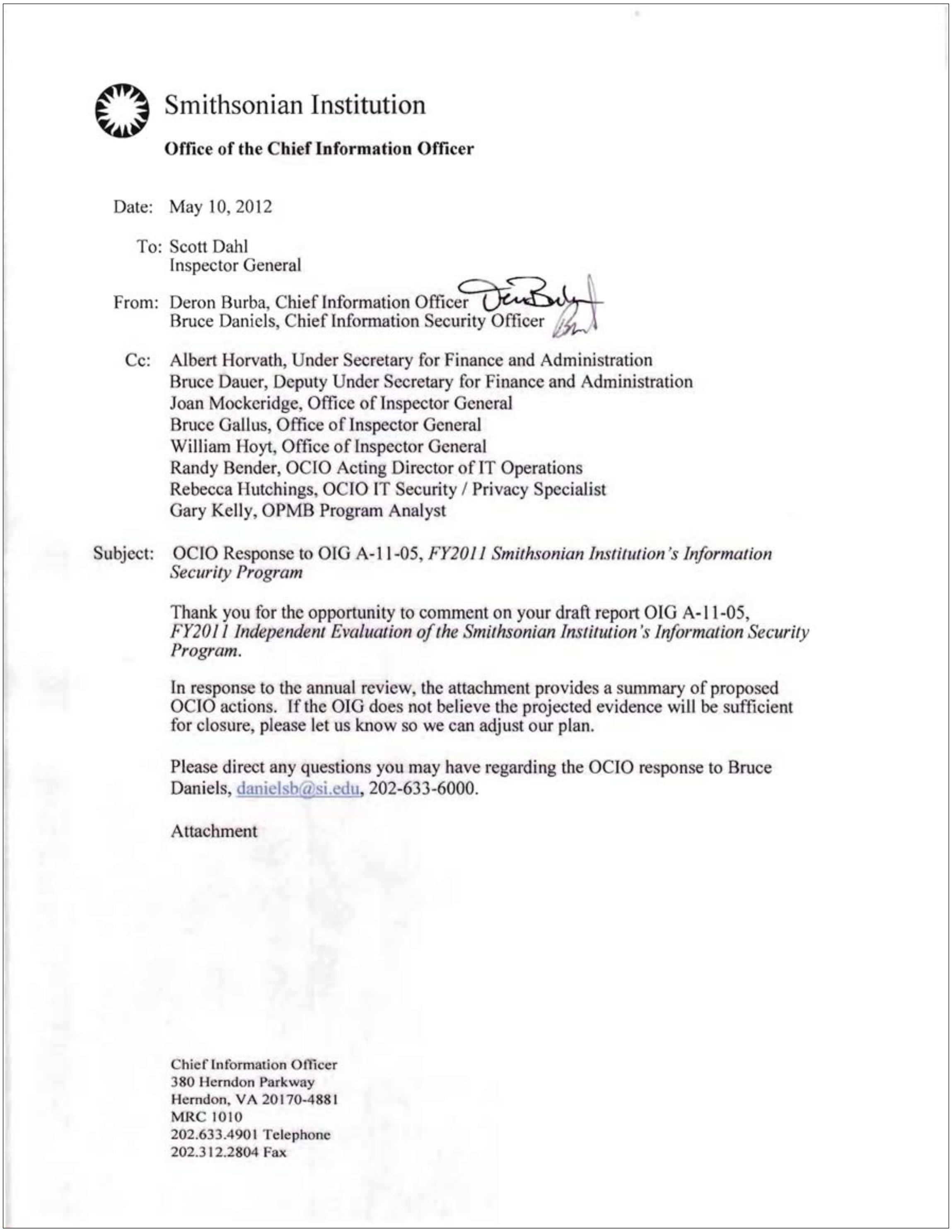
Report	Date Issued	Recommendation	Current Status
		Engage personnel with expertise and knowledge of Smithsonian information systems and processes including representatives from the Offices of the Undersecretaries and the Chief Information Officer, Unit and Museum Directors, and the Smithsonian Privacy Officer in reviewing the updates to the policies and documents and in the resulting modifications to the Smithsonian's FISMA inventory.	Target date 9/15/2012
		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 9/15/2012
		Update TSG 930-02 Security Controls Manual (PM-5) to reflect the approved management process.	Target date 9/15/2012
		We recommend that SI 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 9/15/2012

The following table represents the current status of the prior years' privacy program recommendations, eight (8) open recommendations and one (1) closed recommendation in FY 2011:

Report	Date Issued	Recommendation	Current Status
Privacy Program Review			
Smithsonian Institution Privacy Program A-08-08	5/29/2009	Develop, document, and implement privacy policies and procedures to support an overall privacy program that adequately addresses privacy-related risks. Additionally, privacy policies and procedures for websites should include practices such as conducting risk assessments, requiring a link to Smithsonian privacy policy, and complying with Smithsonian and federal website privacy requirements.	Target date revised to March 2012 Delayed
		Develop and implement an annual privacy-training program and require all Smithsonian employees and contractors to complete the training.	**Closed**
		Develop, document, and implement a process for identifying and documenting PII used by the Smithsonian. This process should result in a detailed list describing PII by origin, use, format, and location.	Target date 3/15/2012 Delayed
		Establish and implement requirements to reduce holdings of PII to the extent practicable.	Target date revised to March 2012 Delayed
		Develop, document, and implement procedures for conducting PIAs. Procedures for completing PIAs should address relevant Smithsonian requirements.	Target date 3/15/2012 Delayed
		Post completed PIAs on the Smithsonian's public website.	Target date revised to August 2011 Delayed
		Develop, document, and implement policies and procedures for safeguarding documents containing PII.	Target date revised to March 2012 Delayed

Report	Date Issued	Recommendation	Current Status
		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 March 2012. Delayed
		Ensure that privacy links for all Smithsonian web site entries have consistent content and style to ensure compliance with the Smithsonian's published web privacy policy and procedures.	Target date revised to December 2011. Delayed

MANAGEMENT RESPONSE



Smithsonian Institution

Office of the Chief Information Officer

Date: May 10, 2012

To: Scott Dahl
Inspector General

From: Deron Burba, Chief Information Officer
Bruce Daniels, Chief Information Security Officer

Cc: Albert Horvath, Under Secretary for Finance and Administration
Bruce Dauer, Deputy Under Secretary for Finance and Administration
Joan Mockeridge, Office of Inspector General
Bruce Gallus, Office of Inspector General
William Hoyt, Office of Inspector General
Randy Bender, OCIO Acting Director of IT Operations
Rebecca Hutchings, OCIO IT Security / Privacy Specialist
Gary Kelly, OPMB Program Analyst

Subject: OCIO Response to OIG A-11-05, *FY2011 Smithsonian Institution's Information Security Program*

Thank you for the opportunity to comment on your draft report OIG A-11-05, *FY2011 Independent Evaluation of the Smithsonian Institution's Information Security Program.*

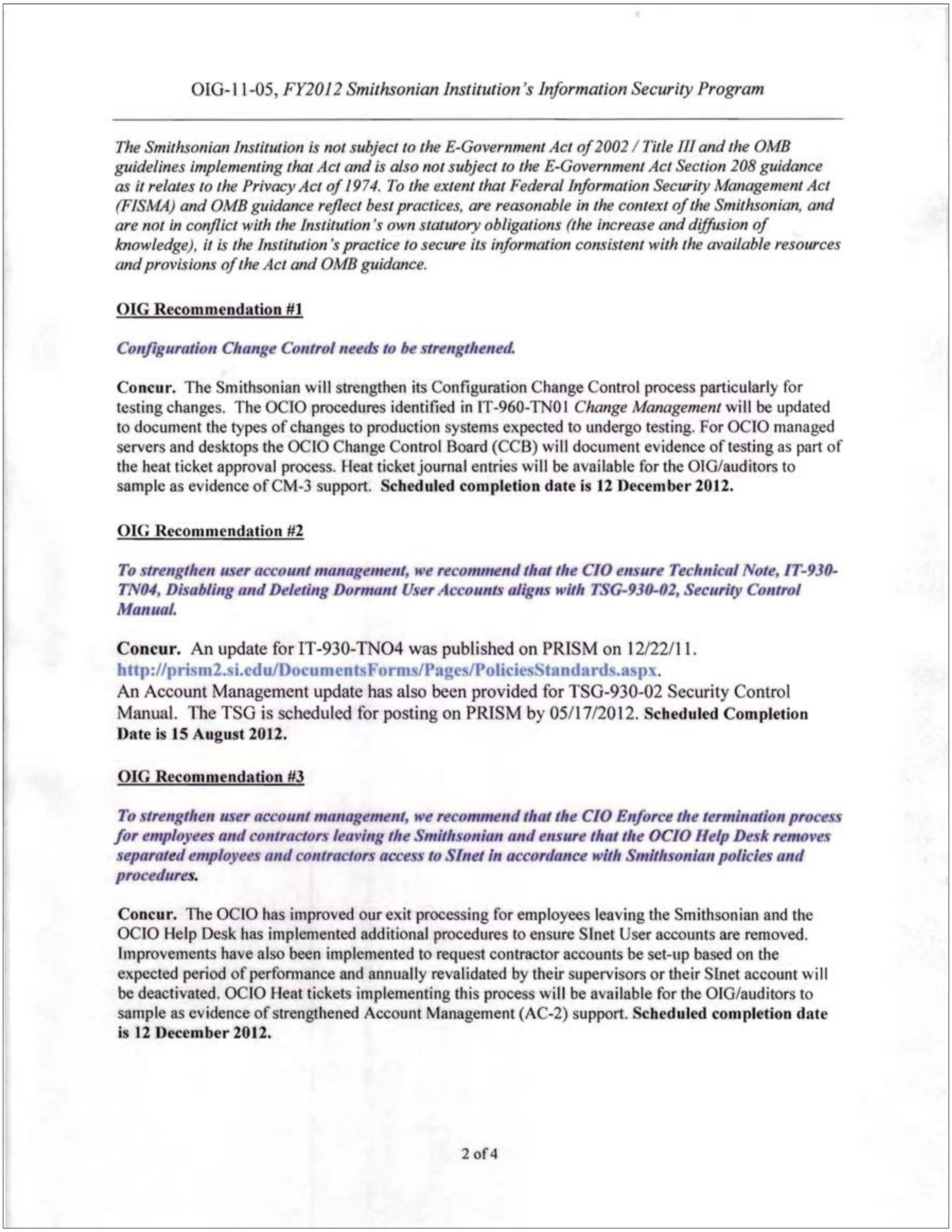
In response to the annual review, the attachment provides a summary of proposed OCIO actions. If the OIG does not believe the projected evidence will be sufficient for closure, please let us know so we can adjust our plan.

Please direct any questions you may have regarding the OCIO response to Bruce Daniels, danielsb@si.edu, 202-633-6000.

Attachment

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

MANAGEMENT RESPONSE (CONTINUED)



OIG-11-05, *FY2012 Smithsonian Institution's Information Security Program*

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

Configuration Change Control needs to be strengthened.

Concur. The Smithsonian will strengthen its Configuration Change Control process particularly for testing changes. The OCIO procedures identified in IT-960-TN01 *Change Management* will be updated to document the types of changes to production systems expected to undergo testing. For OCIO managed servers and desktops the OCIO Change Control Board (CCB) will document evidence of testing as part of the heat ticket approval process. Heat ticket journal entries will be available for the OIG/auditors to sample as evidence of CM-3 support. **Scheduled completion date is 12 December 2012.**

OIG Recommendation #2

To strengthen user account management, we recommend that the CIO ensure Technical Note, IT-930-TN04, Disabling and Deleting Dormant User Accounts aligns with TSG-930-02, Security Control Manual.

Concur. An update for IT-930-TNO4 was published on PRISM on 12/22/11.
http://prism2.si.edu/DocumentsForms/Pages/PoliciesStandards.aspx.
An Account Management update has also been provided for TSG-930-02 Security Control Manual. The TSG is scheduled for posting on PRISM by 05/17/2012. **Scheduled Completion Date is 15 August 2012.**

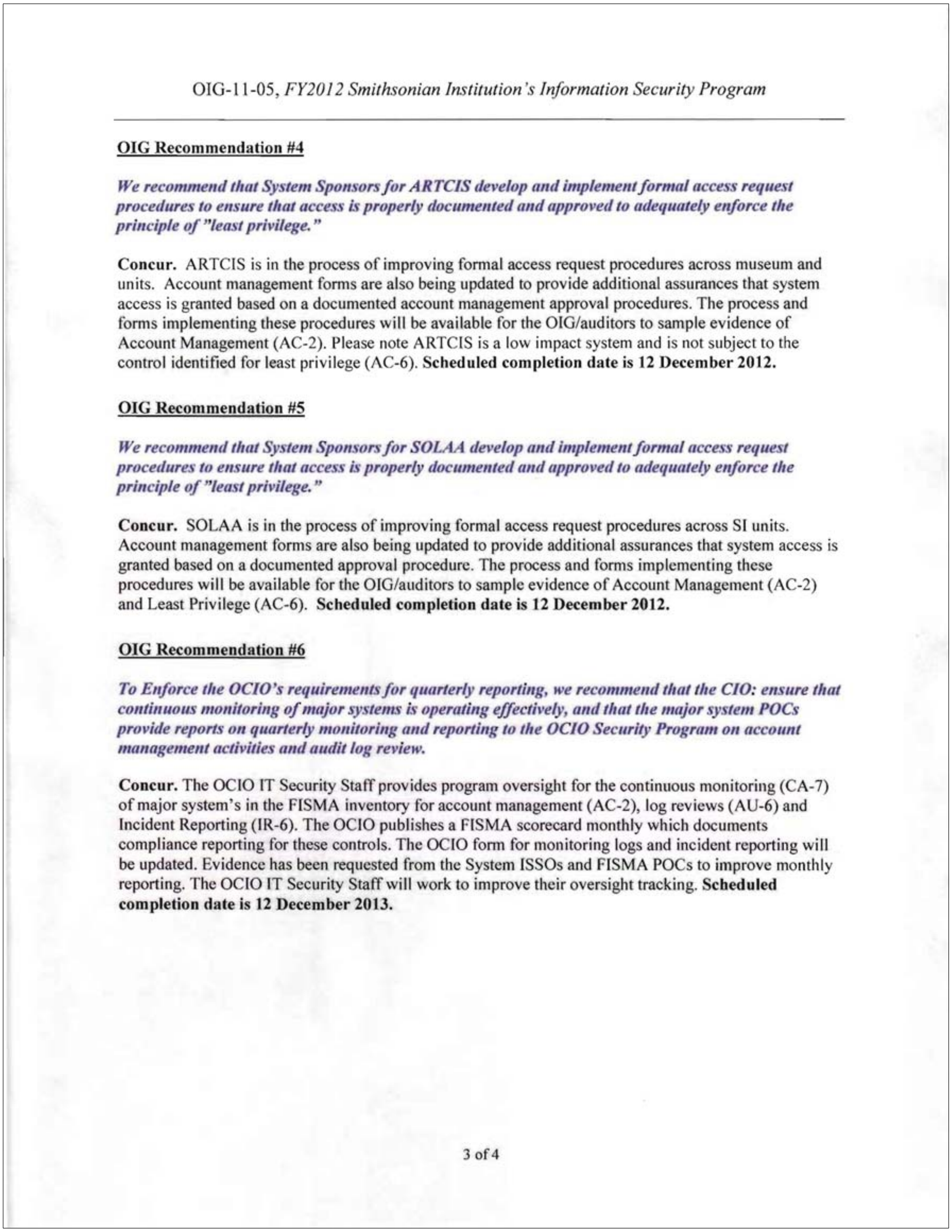
OIG Recommendation #3

To strengthen user account management, we recommend that the CIO Enforce the termination process for employees and contractors leaving the Smithsonian and ensure that the OCIO Help Desk removes separated employees and contractors access to SInet in accordance with Smithsonian policies and procedures.

Concur. The OCIO has improved our exit processing for employees leaving the Smithsonian and the OCIO Help Desk has implemented additional procedures to ensure SInet User accounts are removed. Improvements have also been implemented to request contractor accounts be set-up based on the expected period of performance and annually revalidated by their supervisors or their SInet account will be deactivated. OCIO Heat tickets implementing this process will be available for the OIG/auditors to sample as evidence of strengthened Account Management (AC-2) support. **Scheduled completion date is 12 December 2012.**

2 of 4

MANAGEMENT RESPONSE (CONTINUED)



OIG Recommendation #4

We recommend that System Sponsors for ARTCIS develop and implement formal access request procedures to ensure that access is properly documented and approved to adequately enforce the principle of "least privilege."

Concur. ARTCIS is in the process of improving formal access request procedures across museum and units. Account management forms are also being updated to provide additional assurances that system access is granted based on a documented account management approval procedures. The process and forms implementing these procedures will be available for the OIG/auditors to sample evidence of Account Management (AC-2). Please note ARTCIS is a low impact system and is not subject to the control identified for least privilege (AC-6). **Scheduled completion date is 12 December 2012.**

OIG Recommendation #5

We recommend that System Sponsors for SOLAA develop and implement formal access request procedures to ensure that access is properly documented and approved to adequately enforce the principle of "least privilege."

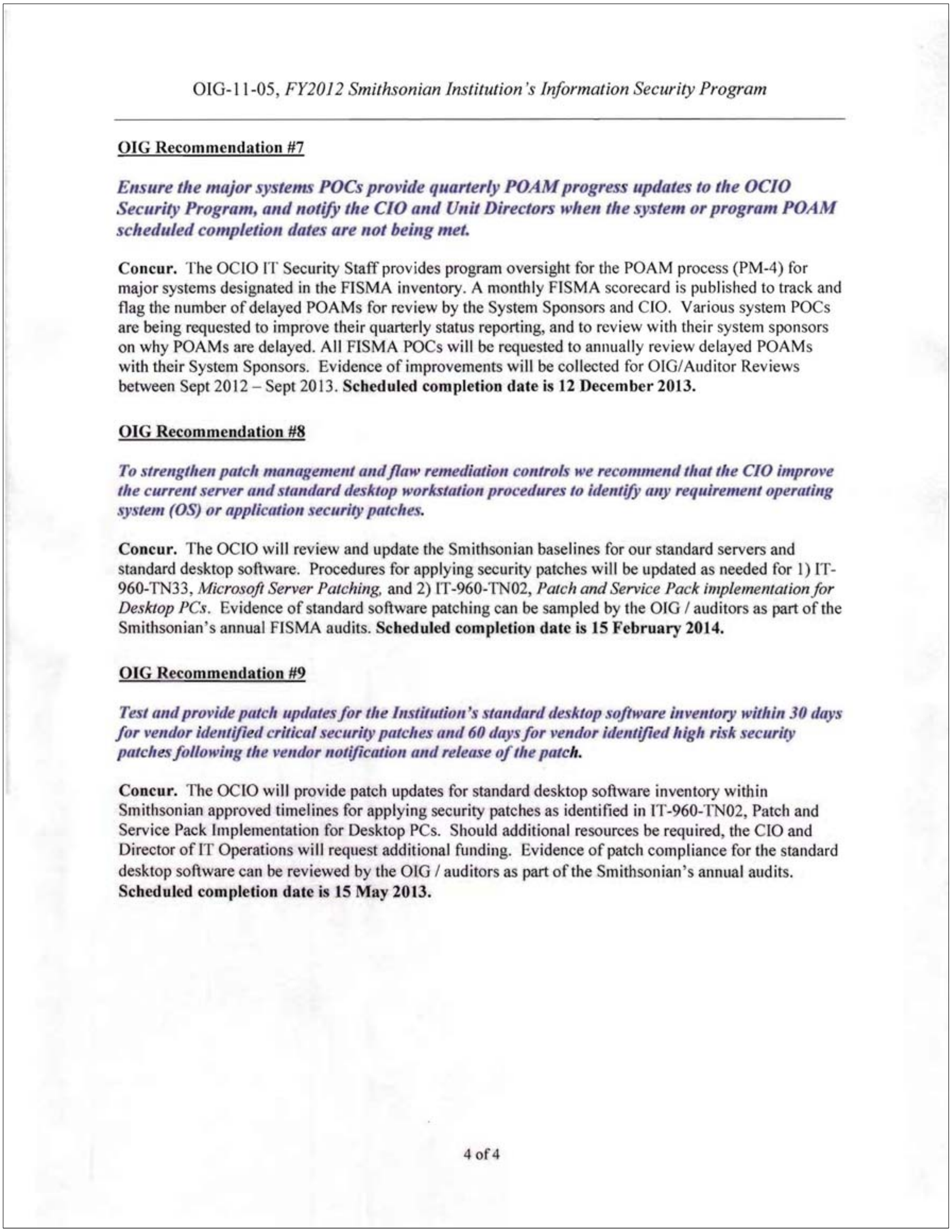
Concur. SOLAA is in the process of improving formal access request procedures across SI units. Account management forms are also being updated to provide additional assurances that system access is granted based on a documented approval procedure. The process and forms implementing these procedures will be available for the OIG/auditors to sample evidence of Account Management (AC-2) and Least Privilege (AC-6). **Scheduled completion date is 12 December 2012.**

OIG Recommendation #6

To Enforce the OCIO's requirements for quarterly reporting, we recommend that the CIO: 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 review.

Concur. The OCIO IT Security Staff provides program oversight for the continuous monitoring (CA-7) of major system's in the FISMA inventory for account management (AC-2), log reviews (AU-6) and Incident Reporting (IR-6). The OCIO publishes a FISMA scorecard monthly which documents compliance reporting for these controls. The OCIO form for monitoring logs and incident reporting will be updated. Evidence has been requested from the System ISSOs and FISMA POCs to improve monthly reporting. The OCIO IT Security Staff will work to improve their oversight tracking. **Scheduled completion date is 12 December 2013.**

MANAGEMENT RESPONSE (CONTINUED)



OIG Recommendation #7

Ensure the major systems POCs provide quarterly POAM progress updates to the OCIO Security Program, and notify the CIO and Unit Directors when the system or program POAM scheduled completion dates are not being met.

Concur. The OCIO IT Security Staff provides program oversight for the POAM process (PM-4) for major systems designated in the FISMA inventory. A monthly FISMA scorecard is published to track and flag the number of delayed POAMs for review by the System Sponsors and CIO. Various system POCs are being requested to improve their quarterly status reporting, and to review with their system sponsors on why POAMs are delayed. All FISMA POCs will be requested to annually review delayed POAMs with their System Sponsors. Evidence of improvements will be collected for OIG/Auditor Reviews between Sept 2012 – Sept 2013. **Scheduled completion date is 12 December 2013.**

OIG Recommendation #8

To strengthen patch management and flaw remediation controls we recommend that the CIO improve the current server and standard desktop workstation procedures to identify any requirement operating system (OS) or application security patches.

Concur. The OCIO will review and update the Smithsonian baselines for our standard servers and standard desktop software. Procedures for applying security patches will be updated as needed for 1) IT-960-TN33, *Microsoft Server Patching,* and 2) IT-960-TN02, *Patch and Service Pack implementation for Desktop PCs*. Evidence of standard software patching can be sampled by the OIG / auditors as part of the Smithsonian's annual FISMA audits. **Scheduled completion date is 15 February 2014.**

OIG Recommendation #9

Test and provide patch updates for the Institution's standard desktop software inventory within 30 days for vendor identified critical security patches and 60 days for vendor identified high risk security patches following the vendor notification and release of the patch.

Concur. The OCIO will provide patch updates for standard desktop software inventory within Smithsonian approved timelines for applying security patches as identified in IT-960-TN02, Patch and Service Pack Implementation for Desktop PCs. Should additional resources be required, the CIO and Director of IT Operations will request additional funding. Evidence of patch compliance for the standard desktop software can be reviewed by the OIG / auditors as part of the Smithsonian's annual audits. **Scheduled completion date is 15 May 2013.**