Description of document:	**FY 2008 Independent Audit of Smithsonian Astrophysical Observatory Scientific Computing Infrastructure (A-08-03), September 30, 2008**
Requested date:	27-December-2009
Released date:	09-April-2010
Posted date:	10-May-2010
Title of document	Smithsonian Astrophysical Observatory Scientific Computing Infrastructure Report Number A-08-03, September 30, 2008
Source of document:	Office of the Inspector General Smithsonian Institution MRC 524 PO Box 37012 Washington DC 20013-0712

Smithsonian Institution

Office of the Inspector General

April 9, 2010

Enclosed is our response to your December 27, 2009 letter, in which you requested "a copy of the segregable releasable portions of Report on Fiscal Year 2008 Independent Audit of Smithsonian Astrophysical Observatory Scientific Computing Infrastructure (A-08-03) dated September 30, 2008." As stated in February 2, 2010 letter, we are releasing the portions of the requested report that are consistent with the principles outlined below.

The Smithsonian Institution and its Office of the Inspector General (OIG) are not subject to the Freedom of Information Act (FOIA), 5 U.S.C. § 552, or the Privacy Act, 5 U.S.C. § 552a. *Dong v. Smithsonian Institution*, 125 F.3d 877 (D.C. Cir. 1997), *cert. denied*, 524 U.S. 922 (1998); Requests for Smithsonian Institution Information, Smithsonian Directive 807 (SD 807) (Feb. 4, 2009). Nevertheless, we provide information to the public in keeping with the Institution's mandate to increase and diffuse knowledge. *See* 20 U.S.C. §41 *et seq.* The Institution and its OIG answer requests for documents consistent with its written policy, SD 807, and adhere to the principles of FOIA, the Privacy Act, and relevant caselaw. In addition, this office must comply with the requirements of the Inspector General Act of 1978, as amended, 5 U.S.C. App. 3, which places restrictions on what information can be released by OIG.

Accordingly, we have redacted the enclosed document consistent with FOIA exemptions 2, which protects from disclosure information relating solely to internal personnel rules and practices of an agency that the divulgence of which would risk the circumvention of a statute or agency regulation, and 6, which protects from disclosure "personnel and medical files and similar files" if such disclosure "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(2) and (6).

You have a right to appeal a partial or full denial of your request. An appeal must be in writing, addressed to the Smithsonian Institution Office of the Inspector General, and made within 60 days from the date of this response letter. The request must explain your reason(s) for the appeal. The Smithsonian Inspector General will decide your appeal in writing specifying the reason(s) for the granting or denying of the appeal.

This completes this office's response to your December 27, 2009 request. Thank you for your interest in the Smithsonian Institution and its Office of the Inspector General.

Sincerely,

Epin H. Christensen
Counsel to the Inspector General

MRC 524
PO Box 37012
Washington DC 20013-7012
202.633.7050 Telephone
202.633.7079 Fax

Smithsonian Institution
Office of the Inspector General

In Brief

SMITHSONIAN ASTROPHYSICAL OBSERVATORY SCIENTIFIC COMPUTING INFRASTRUCTURE

Report Number A-08-03, September 30, 2008

Why We Did This Evaluation

Under the Federal Information Security Management Act of 2002 (FISMA), the Office of the Inspector General conducts an annual independent assessment of the Institution's information security program. As part of that assessment, FISMA requires a review of a subset of information systems. This report covers one such system, SAO Scientific Computing Infrastructure, and evaluates management, operational, and technical security controls.

What We Recommended

We made 14 recommendations to strengthen controls over SAO's infrastructure by enforcing Institution policies, procedures, and practices for (b) (2) updating its system security plan; and (b) (2)

Management concurred with our findings and recommendations and has taken or planned actions that will resolve all our recommendations. Based on improvements already implemented, we are closing 4 of the 14 recommendations.

What We Found

Overall, we determined operational, management, and technical controls for the Smithsonian Astrophysical Observatory (SAO) Scientific Computing Infrastructure were in place and operating effectively. While management has complied with the majority of Smithsonian, Office of Management and Budget, and National Institute of Standards and Technology requirements, we did identify several areas where they need to make improvements. Specifically, we found that:

- OCIO (b) (2) remain out of sync with NIST requirements. Also, SAO did not document in its system security plan any deviations from the Smithsonian (b) (2)
- OCIO was not timely in updating Smithsonian procedures to reflect changes to NIST requirements. Therefore, SAO could not update its system security plan to document these changes.
- SAO management could not ensure that (b) (2)
- (b) (2)
- (b) (2)
- SAO did not require new users to take security awareness training within 30 days, in accordance with Institution policy.
- (b) (2)

Without adequate controls in place to enforce Institution policies, procedures, and practices for the System, the confidentiality, availability, and integrity of the system and the sensitive data it processes may be at greater risk than management is willing to accept.

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

REPORT ON FISCAL YEAR 2008
INDEPENDENT AUDIT OF
SMITHSONIAN ASTROPHYSICAL OBSERVATORY
SCIENTIFIC COMPUTING INFRASTRUCTURE
SMITHSONIAN INSTITUTION
OFFICE OF THE INSPECTOR GENERAL

Cotton & Company LLP
Auditors · Advisors
635 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
703.836.6701
www.cottoncpa.com

CONTENTS

REPORT ON FISCAL YEAR 2008 INDEPENDENT AUDIT OF SMITHSONIAN ASTROPHYSICAL OBSERVATORY SCIENTIFIC COMPUTING INFRASTRUCTURE SMITHSONIAN INSTITUTION OFFICE OF THE INSPECTOR GENERAL

Cotton & Company LLP conducted an audit of the Smithsonian Institution's security management programs and practices to determine the effectiveness of management, operational, and technical security controls over the Smithsonian Astrophysical Observatory (SAO) Scientific Computing Infrastructure, which is the general support system (GSS).

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. Although the E-Government Act of 2002 does not apply to the Institution, the Institution supports the information security practices required by the Act because they are consistent with and advance the Institution's mission and strategic goals.

FISMA outlines federal information security compliance criteria, including the requirement for an annual independent assessment by the Smithsonian's Inspector General. This report provides details of the performance audit of SAO's Scientific Computing Infrastructure's management, operational, and technical security controls, and supports the Smithsonian Institution Office of the Inspector General (OIG) annual FISMA evaluation of the information security controls implemented by the Institution, based primarily on the work performed by Cotton & Company LLP.

BACKGROUND

FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) identify security requirements for federal information security programs. These include:

- **Minimum Security Requirements.** NIST's Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems,* specifies minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies must meet the minimum security requirements, as defined in the standard, through the use of the security controls in accordance with NIST Special Publication (SP) 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems.*

  The use of security controls from NIST SP 800-53 Revision 1, and the incorporation of baseline (minimum) controls as a starting point in the control selection process, facilitates a more consistent level of security in an organizational information system. It also offers the needed flexibility to tailor the controls based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

- **Annual System Security Control Assessments.** NIST's Draft SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems* contains specific control objectives and techniques against which a system can be tested and measured. Performing a security control assessment and mitigating any of the weaknesses found in the assessment is an effective way to determine if the system, or the information it contains, is adequately secured and protected from loss, misuse, unauthorized access, or modification. OMB guidelines require organizations to use the NIST security control assessment guide to evaluate each of their major systems, annually.

- **Certification and Accreditation.** NIST's SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* states that systems should be certified and accredited. A certification is "a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly and operating as intended." Systems accreditation is "the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to operations, assets, or individuals based on the implementation of the agreed-upon set of security controls." Organizations should use the results of the certification to reassess their risks and update system security plans to provide the basis for making security accreditation decisions.

- **System Security Plan (SSP).** NIST's SP 800-18 *Guide for Developing Security Plans for Federal Information Systems,* requires that all major application and general support systems be covered by a security plan. The plan provides an overview of the security requirements of a system and describes controls in place or planned for meeting those requirements. Additionally, the plan defines responsibilities and the expected behavior of all individuals accessing the system. The NIST guide also instructs that the security plan should describe the management, operational, and technical controls the organization has implemented to protect the system. Among other things, these controls include user identification and authentication procedures, contingency/disaster recovery planning, application software maintenance, data validation, and security awareness training.

SAO SYSTEM BACKGROUND

The Smithsonian Astrophysical Observatory Scientific Computing Infrastructure is composed of the following:

- Networking and telecommunications IT infrastructure [redacted (b) (2)]
- Servers [redacted (b) (2)]
- Data storage arrays
- [redacted (b) (2)]
- Desktop computers and scientific workstations.

The users of the system include the staff of the Harvard-Smithsonian Center for Astrophysics (both Harvard and SAO staff), and research collaborators throughout the world.

SAO has placed powerful astronomical instruments in operation that capture enormous amounts of data that must be stored, analyzed, and disseminated. SAO's science mission is highly dependent on high-performance computing and archive servers, as well as on online and near-line storage [redacted (b) (2)] The underlying science mission consists, in part, of:

- Astrophysics research using data gathered by the Multiple Mirror Telescope (MMT) to detect icy comets, asteroids, and moons in the outer solar system; the search for planets in other solar systems; determining the Milky Way's formation history; measuring the distribution of galaxies when the universe was half its present age or less; and quantifying the abundance and characteristics of quasars and their central black holes over the history of the universe.

- Astrophysics research using data gathered by the Submillimeter Array (SMA) imaging instrument to study upper atmosphere circulation and composition in solar system planets and satellites; the formation of planets in nearby stars; the formation of stars in the nearby and distant universe; the structure and nature of the accretion disk around the black hole at the center of our galaxy; and the structure of the most distant galaxies in the universe and how they may differ from those in the nearby universe.

- Astronomical modeling using three-dimensional hydrodynamic simulations of the formation and migration of planets in a disk of circum stellar gas; the evolution of the remaining disk of debris after planets have formed; accretion disks and relativistic jets around black holes; spiral density waves in galaxies, giant molecular clouds, and regions of star formation; and the formation of galaxies, Lyman-alpha clouds, and large-scale structures in the universe.

- [redacted (b) (2)] an expanding array of SAO astronomical data products unique in their wide spectral coverage, including radio wavelengths through optical and infrared wavelengths, and X-ray and gamma-ray wavelengths, in support of the National Virtual Observatory.

In addition to scientific computing and astronomical data processing, most of the day-to-day program activities of SAO scientists, engineers, and administrative and technical support staff depend on a robust, efficient, and securely managed and operated Automated Information System (AIS). These activities include e-mail, document processing, storage and retrieval, voice and video teleconferencing, printing, Web publishing, [redacted (b) (2)] as well as [redacted (b) (2)]

SAO is a large, heterogeneous collection of components and management groups. In particular, certain subsystems are managed by groups or individuals outside the organizational structure of the SAO Computation Facility. The High Energy Astrophysics Division within SAO, and the individual field stations [redacted (b) (2)] These subsystems are managed in a manner that is generally consistent with the SI Security Controls, as well as the provisions of the Security Plan. All of the AIS users have signed the Smithsonian Directive (SD) 931 User Agreement and have agreed to follow the security practices detailed in SD 931. [redacted (b) (2)]

OBJECTIVES, SCOPE, AND METHODOLOGY

On behalf of the OIG, Cotton & Company performed an independent audit of the Smithsonian Astrophysical Observatory Scientific Computing Infrastructure. We conducted this audit in accordance with *Government Auditing Standards*, 2007 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 obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This report is intended to meet the objectives described below and should not be used for other purposes.

The objectives of this independent audit were to evaluate and report on management's identification, documentation, and implementation of SAO management, operational and technical security controls, as required by NIST SP 800-53 Revision 1.

To accomplish these objectives, we performed detailed audit procedures of required controls using suggested audit methods and objectives as outlined in NIST Draft SP 800-53A. We performed a high-level review of available certification and accreditation (C&A) documentation related to the SAO system, including:

- System Security Plan, including Documentation of Specific 800-53 Required Controls
- Plan of Action and Milestones (POA&M)
- Risk Assessment
- Contingency/Disaster Recovery Plans, and
- Certification and Accreditation Letters

Effective July 2007, management classified the SAO general support system as a moderate-impact system in accordance with NIST's FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems.* As a result, we evaluated the SAO's general controls, as of March 21, 2008, using suggested test procedures for a moderate-impact system as defined in NIST's Draft SP 800-53A. Test procedures in SP 800-53A were designed by NIST to test specific security controls outlined in NIST SP 800-53. We tested controls defined by SP 800-53, Revision 1, through interview, observation, and specific testing procedures where applicable. Examples of key controls tested include: administration of user accounts; logging, monitoring, and incident response; segregation of duties; and service continuity controls within the SAO GSS.

RESULTS

Overall, we determined operational, management, and technical controls for the SAO GSS were substantially in place and operating effectively. While management has complied with the majority of Smithsonian, OMB, and NIST requirements we did identify several areas where further improvements are needed.

We believe issues related to (b) (2) are the two most significant issues.

(b) (2)

(b) (2)

(b) (2)

We noted other issues, also included in this report, that we felt were of lesser significance but are still important enough to warrant management attention and remediation.

The following is a more detailed discussion of the weaknesses we found as well as recommendations for strengthening management controls over the SAO GSS. We present our findings in the order of greatest risk to the system.

(b) (2)

(b) (2)

(b) (2)

- (b) (2)
- (b) (2)
- (b) (2)
- (b) (2)
- (b) (2)

(b) (2)

(b) (2)

Recommendation

1. We recommend that the system sponsor [redacted]

Controls are not adequate to ensure that the organization [redacted] We currently have an open recommendation on the [redacted] issue with OCIO. Further, SAO has not documented instances where suggested security controls in the Smithsonian [redacted] were not implemented due to [redacted] or valid business reasons.

In addition, [redacted]

Recommendation

2. We recommend that the system sponsor comply with [redacted (b) (2)] In addition, management should fully document all instances where [redacted (b) (2)] are not followed, due to [redacted (b) (2)] or valid business reasons, and this documentation should reflect management acceptance of associated risks.

SAO System Security Plan Was Not Updated

Controls are not adequate to ensure that the SAO SSP is reviewed and updated in accordance with OMB and NIST policy. Specifically, at the time of our fieldwork the SSP had not been updated to reflect new requirements outlined in NIST SP 800-53 Revision 1. NIST SP 800-53 Revision 1 was made final in December 2006 and provided agencies with a 1-year grace period to implement new or modified control requirements. Our review of the SSP noted these new requirements had not yet been addressed.

Examples where controls were not documented in the SSP included:

- [redacted (b) (2)]
- [redacted (b) (2)]
- [redacted (b) (2)]

Per discussions with management, we determined OCIO is responsible for updating Smithsonian policy with new requirements from OMB and NIST. Once Smithsonian policy has been updated with the new requirements, OCIO pushes the new requirements down to system sponsors for implementation. We noted OCIO did not update Smithsonian policy requiring implementation of 800-53 Revision 1 controls until November 2007 (one month before the deadline).

In addition, we noted one instance where the SSP incorrectly identified a moderate control as being required for only high systems. The SSP incorrectly stated that the [redacted (b) (2)]

NIST SP 800-53 Revision 1, *Schedule for Compliance with NIST Standards and Guidelines* states, "For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST."

Weak controls for ensuring system security plans are updated to reflect new requirements identified by OMB and NIST, in a timely manner, can increase management's susceptibility to new or emerging risks. Additionally, weak controls for ensuring SSPs are updated in a timely manner results in non-compliance with FISMA.

By the time we conducted our exit conference in August 2008, SAO had updated its SSP to address the new requirements.

Recommendations

We recommend that the CIO:

3. Develop, document, and implement controls to ensure Smithsonian policy is updated timely to include new IT requirements and disseminated to system sponsors and contractors.

4. Ensure system sponsors implement NIST, OMB, and Smithsonian requirements within required timeframes.

(b) (2)

(b) (2)

(b) (2)

The (b) (2) settings are designed to help prevent (b) (2)
Configuring (b) (2)
increases the risk that unauthorized individuals will be able to (b) (2)
SAO network and data. Industry best practices suggest (b) (2)

Recommendation

5. We recommend the system sponsor comply with Smithsonian policy and enforce (b) (2)

(b) (2)

Controls are not adequate to ensure all machines on the SAO GSS (b) (2)

(b) (2)

(b) (2)

(b) (2)

Recommendation

6. We recommend the system sponsor implement (b) (2)

(b) (2)

Controls are not adequate to ensure SAO (b) (2)

(b) (2)

Recommendation

7. We recommend that the system sponsor adhere to Smithsonian policy and (b) (2)

(b) (2)

Controls are not in place to ensure that the organization employs (b) (2)

Per discussions with SAO management we determined (b) (2)

(b) (2)

(b) (2)

The lack of (b) (2) such as (b) (2) increases the risk of (b) (2) by unauthorized or unknown individuals would (b) (2)

[redacted] and increase the likelihood of confidentiality, availability, and integrity of SAO components and data being compromised.

Recommendation

8. We recommend that the system sponsor research tools that will enable [redacted] If management cannot identify [redacted] management should document this deficiency in their risk assessment and system security plan. In addition, if [redacted] cannot be implemented, management should identify compensating controls that will reduce risks associated with [redacted]

New User Security Awareness Training Process Is Inconsistent with Smithsonian Policy

Controls are not adequate to ensure the organization provides basic security awareness training to all information system users (including managers and senior executives) within 30 days after hire. Specifically, we found through interviews with SAO that security awareness training is not required when new users are added. Instead, security awareness training is only provided on an annual basis. We did note that management stated that SAO is currently revising their policy and implementing requirements for new hires to receive training within the first 30 days of hire.

SAO is not currently following Smithsonian policies outlined in IT-930-02. SAO has not fully assessed the risks associated with allowing users and employees on networks before they have received security awareness training.

IT-930-02 *Security Controls Manual* states, "Directors of each museum, research center, or office will ensure that new employees, volunteers, interns, visiting scholars and contractor personnel complete the course within 30 days after beginning work."

Without an effective security awareness training program in place, which ensures first-time users complete security awareness training in accordance with Smithsonian policy (within 30 days of access or sooner), the likelihood of inappropriate or unauthorized activities occurring that can negatively affect confidentiality, availability, or integrity of systems and data, increases. In addition, where management relies on users to follow policies that are not enforced by automated mechanisms, the lack of adequate user training reduces the effectiveness of these controls.

Recommendation

9. We recommend that the system sponsor adhere to Smithsonian policies and provide security awareness training to all staff within 30 days of hire.

Controls Over the Primary and Alternate Processing Facilities Are Not Adequate

Controls over the primary and alternate processing/storage facilities do not meet Institution and NIST requirements. Specifically, we noted the following weaknesses related to the primary and alternate processing facilities located in (b) (2)

- (b) (2)

  (b) (2)

  (b) (2)

  (b) (2)

  In addition, (b) (2)

Without effective automated controls in place to identify (b) (2) risks to the confidentiality, availability, and integrity (b) (2) are increased.

- (b) (2)

  (b) (2)

  (b) (2)

- (b) (2)

  (b) (2)

(b) (2)

In addition, (b) (2)

The lack of (b) (2) makes it difficult to relate (b) (2).

- Emergency lighting is not in place in the computer room at (b) (2) Currently, the SAO network team employs flashlights in the event of power failures.

  IT 930-02 states: "All systems must meet the following requirements - The SI unit responsible for the computer facility must employ and maintain automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes."

  In addition, NIST SP 800-53 PE-11 states, "The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes."

The lack of emergency lighting can be hazardous to the safety of personnel and equipment in the computer rooms during a power outage. While flashlights do provide some emergency lighting, they are extremely susceptible to failure.

Recommendations

To improve controls over the primary and alternate processing facilities, we recommend that the system sponsor:

10. Follow NIST and Smithsonian requirements for (b) (2) and (b) (2) in a centrally located area. Additionally, the system sponsor needs to (b) (2)
11. (b) (2)
12. (b) (2)
13. (b) (2)
14. Implement emergency lighting in the computer rooms at (b) (2)

SUMMARY OF MANAGEMENT RESPONSE

Management's September 22, 2008, response to our draft report generally concurred with our findings and recommendations. Management's planned actions are summarized below:

Recommendation 1. Concur. SAO will [redacted] By September 5, 2009, management will identify network equipment and staff needed to fully implement [redacted]

Recommendation 2. Concur. OCIO [redacted] requirements for specific types of systems, such as [redacted] SAO agreed to document any deviations [redacted] by July 15, 2009.

Recommendation 3. Concur. OCIO Information Technology Security Staff is responsible for incorporating updates to NIST policy and communicating these updates and compliance timelines to the system sponsors. OCIO acknowledges that timely updates to Institution policies are necessary to allow units the time to implement the necessary changes. OCIO will revise the IT-930-01 *AIS Security Planning Technical Standard and Guideline* to include OCIO's own expectations for incorporating major updates from NIST and OMB into IT-930-02 *Security Controls Manual*. OCIO will publish these revision by December 15, 2008.

Recommendation 4. Concur. OCIO plans to review and update IT-930-02 Appendix E, refine unit reporting requirements to OCIO, and implement unit-scorecards to track and enforce compliance. The new Appendix will be published by December 15, 2008, and units will begin reporting in January 2009. OCIO established a target completion of June 15, 2009 allowing time to monitor unit progress.

Recommendations 5 and 6. Concur. SAO implemented the [redacted] However, the current required settings [redacted] Also, SAO will implement, test, and update the system security plan [redacted] Both actions will be completed by July 15, 2009.

Recommendation 7. Partial Concur. In accordance with SAO system security plan, SAO [redacted] All servers and clients over the past 10 years have [redacted] SAO will provide a copy of its letter from OCIO granting an exception to Institution policy.

Recommendation 8. Concur. By November 15, 2009 management will review [redacted]

Recommendations 9 and 10. Concur. SAO continues to target full compliance with Smithsonian security awareness training policies for all staff with SInet accounts. New SInet users are automatically tracked for completion of training. Additionally, SAO will document in its system security plan requirements to [redacted] These actions will be completed by July 15, 2009.

Recommendation 11. Concur. Management converted [redacted]

Recommendation 12. Concur. Both OCIO and SAO are in discussions about using the [redacted] as [redacted]. SAO will research [redacted] requirements and cost considerations by Jul 15, 2009, and report on their decision.

Recommendation 13. Concur. SAO implemented [redacted] which according to the Computation Department Manager will be reviewed monthly.

Recommendation 14. Concur. SAO believes that the emergency lighting from the hall has historically been sufficient for supporting computer room activities during power failures. Additionally, backup batteries will be stored in the computer room.

OFFICE OF THE INSPECTOR GENERAL COMMENTS

Management has taken and planned actions that respond to all our recommendations, and we consider them resolved. In evaluating management's response to this report, we held several discussions with the Computation Facility Department Manager in an effort to clarify and close several recommendations. We verified that OCIO signed a waiver granting SAO an exception for its [redacted] Through photographs we verified that SAO has installed [redacted] Also, SAO has implemented [redacted] We understand that the Computation Facility Department Manager will conduct a monthly review [redacted] Finally, SAO updated its system security plan Appendix B *Risk Assessment Report*, in which management accepts the risk of a lack of emergency lighting inside the data center. Management believes that the emergency lighting coming from the hall provides adequate illumination of the data center through the glass walls. Based on these actions, we will close recommendations 7, 11, 13, and 14.

Regarding recommendation 9, security awareness training requirements cover all employees whether SInet users or not. Therefore, we do not believe a waiver is warranted.

Concerning recommendation 12, whether it is too costly to have OCIO's [redacted] We do not think granting a waiver is in the best interest of SAO or the Institution as a whole.

We appreciate the courtesy and cooperation of Smithsonian representatives during this audit. If you have any questions concerning this report, please call Joan Mockeridge at 202.633.7050.

Appendix I – Management Comments

Smithsonian Institution Memo

Date: September 22, 2008

To: A. Sprightley Ryan, Inspector General

Cc: Joan Mockeridge
Van L. McGlasson
Bruce Daniels

From: Charles Alcock, Acting Under Secretary for Science, and Director of the Harvard-Smithsonian Center for Astrophysics

Ann Speyer, Chief Information Officer

Subject: Response to OIG Draft Audit Report Number A-08-03, *Smithsonian Astrophysical Observatory's Scientific Computing Infrastructure Audit*

Thank you for the opportunity to comment on the draft audit report on the Smithsonian Astrophysical Observatory's (SAO) Scientific Computing Infrastructure. SAO and the OCIO have jointly reviewed the draft report and our responses to the audit findings and recommendations are provided below.

For those recommendations which we have completed actions, a separate letter will be provided to the OIG with evidence requesting the recommendation be closed.

Please direct any questions you may have regarding the SAO response to Van L. McGlasson, SAO Computation Facility Department Manager, at (b) (6). Questions about the OCIO response should be directed to Bruce Daniels, OCIO Computer Security Director, at 202-633-6000.

OIG Recommendation No. 1

We recommend that the system sponsor (b) (2) (b) (2)

Concur. SAO has opened a POA&M to (b) (2) (b) (2) SAO will identify the network equipment and staff necessary to fully implement (b) (2) (b) (2) The target date for completing these activities and requesting this POA&M be closed is September 5, 2009.

The Castle, Room 230
1000 Jefferson Drive SW
Washington DC 20560-0009
(202) 633-5135 Telephone
(202) 633-8942 Fax

OIG Recommendation No. 2

We recommend that the system sponsor comply with (b) (2) (b) (2) *In addition, management should fully document all instances where suggested* (b) (2) *are not followed, due to* (b) (2) *or valid business reasons, and this documentation should reflect management acceptance of associated risks.*

Concur. SAO maintains (b) (2) as required by (b) (2) SI OCIO currently publishes (b) (2) documentation requirements for:

- (b) (2)

A POA&M will be opened by SAO to fully document instances where suggested (b) (2) (b) (2) are not being followed based on SI published (b) (2) The documentation of (b) (2) will be provided to the OIG, and will identify this evidence as SAO's management acceptance of associated risks. The target date for completing these activities and requesting this POA&M be closed is July 15, 2009.

OIG Recommendation No. 3

We recommend that the CIO develop, document, and implement controls to ensure Smithsonian policy is timely updated to include new IT requirements and disseminated to system sponsors and contractors.

Concur. As noted in the audit, OCIO ITSS is responsible for translating NIST policy into SI policy and general procedures and communicating these updates and compliance timelines to the Unit's system sponsors, IT Directors and Information System Security Officers (ISSOs). The OCIO acknowledges that updated Smithsonian policies and procedures need to be in place and disseminated in time to allow units time to implement. A POA&M will be opened by the OCIO to draft an update to incorporate an implementation requirement timeline in the AIS Security Planning Technical Standard & Guideline (IT-930-01). The update will identify OCIO own expectations for incorporating major updates from NIST and OMB into SI Security Controls Manual (IT-930-02) for dissemination. The updated policy and procedures will be reviewed with the OCIO office, Computer Security Advisory Committee (CSAC) and Units by November 15, 2008. Once the policy and procedures are published (IT-930-01/IT-930-02), the OIG will be requested to close this POA&M. A target completion date to publish these updates is

identified as December 15, 2008.

OIG Recommendation No. 4

We recommend that the CIO Ensure system sponsors implement NIST, OMB, and Smithsonian requirements within required timeframes.

Concur. The OCIO is planning to review and update the Technical Standards & Guidelines (IT-930-02) Appendix E to refine Unit reporting requirements to the OCIO. An updated Appendix is expected to be published by December 15, 2008, and the Units will begin reporting starting in January 2009. The target date for completing these POA&M activity is June 15, 2009.

OIG Recommendation No. 5

We recommend the system sponsor comply with Smithsonian policy and enforce (b) (2) (b) (2) (b) (2)

Concur. SAO has implemented the appropriate (b) (2) settings as specified in the OCIO (b) (2) however, please note that the currently required settings (b) (2) SAO researched this control and currently believes the (b) (2) (b) (2) A POA&M will be opened to further research (b) (2) (b) this requirement. The target date for completing the implementation and test of this control is July 15, 2009.

OIG Recommendation No. 6

We recommend the system sponsor implement (b) (2) (b) (2) (b) (2)

Concur. SAO will implement, test, and update SSP documentation on (b) (2) settings for (b) (2) as specified in the (b) (2) (b) (2) The target date for completing this POA&M activity is July 15, 2009.

OIG Recommendation No. 7

We recommend that the system sponsor adhere to Smithsonian policy and (b) (2) (b) (2)

Partial-concur. As identified in the SAO System Security Plan, SAO's supports its own (b) (2) on its SAO network infrastructure. All SAO servers and clients over the past 10 years (b) (2) SInet (b) (2)

(b) (2) (b) (2) SAO is not required by the Smithsonian to use the SI (b) (2) SAO will provide the OIG with a copy of an SI OCIO granted exception, and request this recommendation be closed. No POA&M will be opened.

OIG Recommendation No. 8

We recommend that the system sponsor research tools that will enable (b) (2) (b) (2) (b) (2) *If management cannot identify* (b) (2) *management should document this deficiency in their risk assessment and system security plan. In addition, if* (b) (2) *cannot be implemented, management should identify compensating controls that will reduce risks associated with* (b) (2)

Concur. SAO will open a POA&M. SAO will review (b) (2) requirements for (b) (2) that can support (b) (2) (b) (2) (b) (2) The target date for completing this POA&M activity is November 15, 2009.

OIG Recommendation No. 9

We recommend that the system sponsor adhere to Smithsonian policies and provide security awareness training to all staff within 30 days of hire.

Concur. SAO continues to target full compliance with the Smithsonian security awareness training policies for all SAO staff who have been granted an SI network account. Each SI network account holder is automatically tracked for security awareness training within 30 days of receiving their IT account.

The target date for completing these activities and requesting this POA&M be closed is July 15, 2009. A waiver of computer security awareness training is expected to be requested for SAO staff who do not require access to an SI account.

OIG Recommendation No. 10

We recommend that the system sponsor follow NIST and Smithsonian requirements for (b) (2) *and* (b) (2) *Additionally, the system sponsor needs to* (b) (2)

Concur. The SAO Scientific Computing Infrastructure currently provides support to allow for the (b) (2) In order to ensure (b) (2) (b) (2) a POA&M will be opened to document in the SAO System

Appendix I – Management Comments

Security Plan that SAO schedules, performs, documents, and reviews requirements for (b) (2) (b) (2) SAO will implement procedures to (b) (2) (b) The target date for completing these activities and requesting this POA&M be closed is July 15, 2009.

OIG Recommendation No. 11

We recommend that the system sponsor (b) (2) (b) (2)

Concur. SAO has completed the conversion identified in this recommendation. The OIG will be provided with a separate letter and evidence to request this recommendation be closed. No POA&M will be opened.

OIG Recommendation No. 12

We recommend that the system sponsor (b) (2) (b) (2)

Concur. SAO is working with OCIO to investigate the option of (b) (2) (b) (2) A POA&M will be opened to summarize SAO (b) (2) requirements and cost considerations. The OIG will be provided with a separate letter which documents the SAO Unit Director acceptance of this risk and an OCIO exception request will be submitted based on SAO cost considerations. Once the SAO requirements and costs are documented, and if the waiver is approved the POA&M will be closed. A target completion date is July 15, 2009.

OIG Recommendation No. 13

We recommend that the system sponsor (b) (2) (b) (2) (b) (2)

Concur. SAO has added a (b) (2) the SAO data center as identified in this recommendation. SAO will review (b) (2) (b) (2) The SAO Computation Facility Department Manager is required to periodically (b) (2) (b) (2) The Data Center Manager and staff will be notified that (b) (2) (b) (2) SAO and Smithsonian authorities (b) (2) (b) (2) A POA&M will be opened with a target completion date of February 15, 2009.

Appendix I – Management Comments

OIG Recommendation No. 14

We recommend that the system sponsor implement emergency lighting in the computer room.

Concur. SAO is currently provided with emergency lighting from outside the glass walls of the computer room. This lighting has historically been sufficient for supporting computer room activities during power failures. Additionally backup batteries will be stored in the computer room. The OIG will be provided with a separate letter which documents SAO acceptance of this risk and an OCIO approved exception based on an SAO limited cost benefit justification. No POA&M will be opened.