Smithsonian Institution

Memo

Office of the Inspector General

Date August 10, 2007

To Cristián Samper K., Acting Secretary

Cc Sheila P. Burke, Deputy Secretary and Chief Operating Officer
Ann Speyer, Chief Information Officer
James D. Douglas, Director, Office of Human Resources
Bruce Daniels, Director of IT Security and Smithsonian Computer Security Manager

From A. Sprightley Ryan, Inspector General JSR

Subject Report on the Fiscal Year 2006 Smithsonian Institution Network (SInet) Audit, Number A-06-07

Attached please find a copy of our final report on the FY 2006 FISMA audit of SInet. We made 17 recommendations to strengthen controls over SInet by enforcing Institution policies, procedures, and practices over the confidentiality, availability, and integrity of Institution systems. Management generally concurred with 15 of the recommendations, and we were able to close two of those based on management's actions. Management non-concurred with two recommendations related to our finding that SInet's risk assessment does not meet the basic requirements of NIST 800-30. To resolve these two recommendations, we will meet with OCIO to help develop a model risk assessment.

Please call Stuart Metzger or Joan Mockeridge at 202-633-7050 if you have any questions.

MRC 1204
PO Box 37012
Washington DC 20013-7012
202.633.7050 Telephone
202.633.7079 Fax

AUDIT REPORT

Fiscal Year 2006 Smithsonian Institution Network (SINet) Audit

Number A-06-07

August 10, 2007

Smithsonian Institution

Office of Inspector General

Smithsonian Institution
Office of the Inspector General

In Brief

Smithsonian Institution Network
Report Number A-06-07, August 10, 2007

Why We Did This Evaluation

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

What We Recommended

We made 17 recommendations to strengthen controls over SInet by enforcing Institution policies, procedures, and practices over network account administration, segregation of duties, and risk assessments.

Management generally concurred with the report's findings and recommendations, with the exception of those relating to weaknesses in the development of the SInet risk assessment.

What We Found

The Smithsonian Institution's general support system, SInet, consists of routers, switches, access servers, file servers, mail servers, domain name servers, intrusion detection systems, firewalls, and network monitoring systems.

Management, operational, and technical controls over SInet were not adequate. Our audit noted that the Institution operates in a decentralized environment where responsibility for both performing functions and enforcing IT controls has been assigned to the same individuals. Furthermore, because responsibility for administration and security of SInet has not been centralized under the Office of the Chief Information Officer (OCIO), IT security policies and procedures documented by OCIO have not been consistently implemented or followed. Specifically, we found that:

- Because of weaknesses over the administration of network accounts, management cannot ensure that unauthorized individuals do not have access to SInet or that resources residing on it are obtained through the use of legitimate accounts.
- Vendor patches and fixes to the network operating system for known vulnerabilities need to be installed more timely to reduce the risk of successful intrusions, sabotage, and theft or destruction of critical or sensitive data.
- Management has not enforced proper separation of administrative and security functions and therefore cannot ensure that individuals with high-level or sensitive access to the system will not perform unauthorized activities.
- Risk assessments performed by the Institution did not adequately address the risk and magnitude of harm that could result from unauthorized access to or the unauthorized use, disclosure, disruption, modification, or destruction of information and systems that support the operations and assets of the Institution. Consequently, management cannot fully assess and prioritize all potential threats and vulnerabilities.

Without adequate controls in place to enforce Institution policies, procedures, and practices over SInet, the confidentiality, availability, and integrity of Institution information systems and related data may be at greater risk than management is willing to accept.

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

REPORT ON
FISCAL YEAR 2006 INDEPENDENT AUDIT OF THE SMITHSONIAN INSTITUTION'S NETWORK (SINET)

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

CONTENTS

REPORT ON FISCAL YEAR 2006 AUDIT OF THE SMITHSONIAN INSTITUTION'S NETWORK (SINET)

Cotton & Company LLP conducted an audit of the Smithsonian Institution's network (SInet) security management program and practices to determine the effectiveness of management, operational, and technical controls over the Institution's general support system.

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 Institution's Inspector General. This report covers the evaluation of the SInet security management practices and controls and supports the Smithsonian Institution Office of the Inspector General (OIG) annual FISMA evaluation of the information security controls implemented by the Institution.

BACKGROUND

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

- **Annual System Self-Assessments**. NIST's *Security Self Assessment Guide for Information Technology Systems* contains specific control objectives and techniques against which a system can be tested and measured. Performing a self-assessment and mitigating any of the weaknesses found 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 self-assessment tool annually to evaluate each of their major systems.

- **Certification and Accreditation.** NIST's *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." NIST guidance also discusses system accreditation, which is "the official management decision 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.** NIST's *Guide for Developing Security Plans for Information Technology 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.

OBJECTIVES, SCOPE, AND METHODOLOGY

On behalf of the OIG, Cotton & Company performed an independent audit over SInet, the Institution's general support system. We conducted this audit in accordance with *Government Auditing Standards*, 2003 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.

SInet is composed of routers, switches, access servers, file servers, mail servers, domain names servers, intrusion detection systems, firewalls, and network monitoring systems. This system is located throughout the SI campus in almost every building, from large museum facilities to animal houses at the National Zoo. The network spans 5 states, the District of Columbia, and one foreign country (Panama).

The objectives of this independent audit were to evaluate and report on the existence and effectiveness of management, operational and technical security controls over SInet and to determine if required baselines had been adequately documented and implemented. We evaluated SInet general controls as of August 31, 2006, using NIST's Special Publication (SP) 800-53A, "*Guide for Assessing the Security Controls in Federal Information Systems*," which applies to security controls defined in NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems.*" We tested NIST SP 800-53 general controls through interviews, observation, and specific testing procedures where applicable.

In addition we completed detailed audit procedures for SInet technical controls securing the Institution's border firewall, routers, and use of wireless technologies. Our detailed audit procedures for SInet technical controls included carrying out:

- External and internal penetration testing procedures
- External and internal vulnerability assessment procedures
- Wireless review to determine where the Institution was using wireless and whether wireless access points were adequately secured.

RESULTS

Management, operational, and technical controls over the Institution's general support system were not adequate. Our audit of the Institution's general support system noted that the Institution operates in a decentralized environment where responsibility for both performing functions and enforcing IT controls has been assigned to the same individuals. Responsibility for administration and security of SInet has not been centralized under the Office of the Chief Information Officer (OCIO) and, as a result, IT security policies and procedures documented by OCIO have not been consistently implemented or followed. Without adequate controls in place to enforce Institution policies, procedures, and practices over SInet the confidentiality, availability, and integrity of Institution systems and related data may be at greater risk than management is willing to accept. Specific control weaknesses are detailed below.

Network Account Administration Procedures are Weak

Controls over the administration of SInet accounts are not adequate. Responsibility for adding, deleting, and maintaining SInet accounts has been assigned to various administrators across the Institution, and system administrators are not managing SInet accounts in accordance with Institution or NIST policy. The decentralized administration of SInet contributes to accounts being maintained in an inconsistent manner. In addition, because OCIO does not centrally administer accounts for SInet, they were not performing any periodic reviews of active SInet accounts to ensure these accounts are appropriate.

SInet administrators are responsible for reviewing SInet accounts and reporting results of their reviews to the Computer Security Manager in OCIO in the Dormant Account Monthly Compliance Report. We reviewed the reports submitted to OCIO for May and June 2006 and noted that the reports did not include adequate information on administrators' account reviews.

OCIO's Technical Standard & Guideline IT-930-02 *Security Controls Manual* section 3.1.2 *User Account Management* states:

> System administrators are responsible for reviewing accounts once every 30 days to identify accounts that have been inactive for 30 days. System administrators will disable accounts that have been inactive for 30 days. System administrators will notify the local manager that the account has been disabled and will be deleted after another 150 days (for a total of 180 days of inactivity) unless the manager requests that the account be re-enabled.

Our review of SInet accounts listed as active noted that:

a. Active SInet user accounts totaled 8,116, of which 2,191 (or 27 percent) have been idle in excess of 180 days.

- 51 user accounts in 2006 had no activity for more than 180 days
- 1,541 user accounts had no activity since 2005
- 179 user accounts had no activity since 2004
- 46 user accounts had no activity since 2003 or earlier
- 374 user accounts show "None Found" for a last logon date

b. Active SInet system accounts (accounts used by the Windows operating system and by services running under Windows) totaled 571, of which 394 (or 69 percent) have been idle in excess of 180 days.

- 9 system accounts in 2006 had no activity for more than 180 days
- 58 system accounts had no activity since 2005
- 45 system accounts had no activity since 2004
- 88 system accounts had no activity since 2003 or earlier
- 194 system accounts show "None Found" for a last logon date

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, section 3.5.2 *(User Administration) under User Account Management* states:

> Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Our audit determined that accounts are not being promptly deleted when users leave the Institution. We selected a random sample of 45 individuals whose employment with the Institution was terminated during fiscal year 2006 and noted that 16 of the 45 (35%) still had active user accounts on the network.

Finally, we determined that access request forms for SInet are not adequately retained and periodically reviewed to ensure a user's current access is still appropriate. SInet user Network/Email request forms are faxed to the OCIO helpdesk and kept in the Helpdesk Expert Automation Tool (HEAT) system as a picture format. When we requested a sample of 45 user authorization forms for review, OCIO was unable to provide the forms. We were informed that forms are searchable only by a requester's name or ticket number. There are no periodic reviews conducted to trace the system permission back to authorization documents.

NIST SP 800-14 Section 3.5.2, *Audit and Management Reviews*, states:

> It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

Without adequate controls over the administration of network accounts, management has no means of ensuring unauthorized individuals do not have access to SInet and the resources residing on it through the use of legitimate accounts. In addition, without an up-to-date and accurate list of authorized users on SInet with supporting access request forms, management's ability to identify unauthorized accounts on the network is diminished.

Recommendations

We recommend that the CIO:

1. Assign responsibility to someone within OCIO for periodically reviewing all SInet system and user accounts to determine whether they are still necessary. For example, periodic reviews should detect active accounts with no activity in the last 180 days or accounts associated with individuals who have recently left the Institution.

2. Develop a policy and procedures for maintaining SInet access request forms in a format which system or security administrators will be able to use for future reviews of network accounts.

3. Centralize administration of SInet accounts for all SInet users within OCIO with the exception of the Office of the Inspector General.[1]

Technical Controls Over SInet Need to be Strengthened

Controls need to be strengthened to ensure that significant technical weaknesses do not exist on SInet. The Institution's Technical Note IT-930-TN14, *Vulnerability Scanning of Networked Devices*, establishes procedures for performing vulnerability scanning of all devices connected to SInet. IT-930-TN14 assigns overall responsibility for vulnerability scanning to the Computer Security Manager and responsibility for fixing identified vulnerabilities to various individuals or groups within the Institution.

Our audit noted that OCIO is performing scans of SInet as required by Institution policy and these periodic scans have identified numerous weaknesses, which OCIO is in the process of addressing. We also performed technical testing (penetration testing and vulnerability assessment) both internally and externally on SInet. During our testing we noted that OCIO appears to have strong controls in place for monitoring unauthorized activities on the network. On several occasions our internal and external scans were identified by OCIO security personnel. In these instances, OCIO cut off our access until security personnel were able to determine our activities were authorized.

Notwithstanding the controls for monitoring unauthorized activities, our internal and external testing of SInet identified the following:

- 273 external vulnerabilities, of which 47 were high risk and 226 were medium risk. Specific areas of external weakness included:

    - RPC service vulnerabilities
    - Web server configuration issues and vulnerabilities
    - Multiple buffer overflows

- 178 internal vulnerabilities, of which 145 were high risk, 33 were medium risk, and no low risk vulnerabilities found across 443 scanned machines. Specific internal areas of weakness identified included:

[1] The OIG should continue to maintain administrative control over its accounts and data to ensure sensitive data obtained during the normal course of business is adequately protected from unauthorized disclosure or modification and to maintain statutory independence.

- Web server configuration issues and vulnerabilities
- Anonymous connections allowed to NetBios
- Inappropriate permissions on important registry keys
- Default SNMP community names and other SNMP related vulnerabilities
- Multiple buffer overflows

In addition, although we were initially identified and blocked by OCIO security during our internal testing, we were eventually able to gain administrative access to machines on SInet. We noted several specific technical weaknesses and have separately communicated them to OCIO.

Many of these weaknesses related to default configurations not being changed when systems were installed or patches and hot fixes not being implemented in a timely manner. Best business practices (derived from NIST, NSA, and industry studies) for securing Windows, Unix, and Novell dictate that certain default configurations and permissions be changed to provide tighter security over the operating system.

During our audit we noted that the Institution has not implemented standard security configuration baselines for SInet. The implementation of baselines would in many cases address weaknesses identified in our audit. In our FY 2006 FISMA evaluation report we recommended that the procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced. Additionally, although the Institution does have a documented policy on patching (Technical Note IT-930-TN08 *Implementing Vendor Software Patches/Fixes*), we determined this policy is not being consistently followed or enforced.

Installation delays of vendor patches and fixes to the network operating system for known vulnerabilities exposes the Institution's network to an increased risk of successful hacker attacks. It also increases the potential for network sabotage, theft of the organization's sensitive financial and personal data, and destruction and corruption of databases. Additionally, these unauthorized activities can occur without detection, resulting in management's reliance on potentially inaccurate and incomplete financial and other information.

Recommendations

We recommend that the CIO:

4. Enforce policies and procedures for ensuring that vendor patches and security hot-fixes are installed in a timely manner.

5. Review results of our technical testing (provided during earlier meetings) to ensure weaknesses identified have been addressed by management or identified in OCIO scans. In addition, ensure critical weaknesses such as the ones identified in the SANS Top-20 are addressed first and lower-level risk items addressed later.

Duties are Not Adequately Segregated

Controls are not adequate to ensure sensitive activities within SInet have been adequately segregated. The SInet system security plan includes a section discussing separation of duties and specifically states:

> Separation of duties is a well established security methodology. Moderate and High impact systems have the following requirements: Applications should be designed, implemented and operated in a manner that supports appropriate separation of duties. This requirement means that the information system enforces separation of duties through assigned access authorizations…Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

We determined management has not enforced proper separation of administrative and security functions. For example, our audit noted individuals responsible for administration of SInet user accounts in many cases who are also responsible for the review of system audit logs. Security best practices do not allow the same individual both to set up new users and review audit logs. Without separation of administration and security functions, management cannot ensure individuals with high-level or sensitive access to the system are not performing unauthorized activities.

Recommendation

6. We recommend that the CIO enforce separation of duty controls noted in the SInet system security plan and specifically segregate system administration roles from security roles.

Warning Banners are Not Consistently Applied

Controls are not adequate to ensure SInet warning banners include language required by the Institution and NIST. Specifically, we determined users currently log onto SInet through Windows 2003, Windows 2000, or Novell. Our review of warning banners for each of these platforms noted that the associated warning banners contained different information and in some cases did not include adequate information to meet requirements outlined in the SInet system security plan or NIST SP 800-53.

We determined that the Windows 2000 and Novell warning banners did not agree with the Windows 2003 warning banner. In addition, our review of Technical Standard Guideline IT-930-02, *Security Control Manual* Appendix C, noted that the suggested warning banner language in IT-930-02 did not address all information identified in NIST SP 800-53 and the SInet system security plan. The SInet system security plan, section AC-8 *System Use Notification*, states:

> A System Use Notification informs potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices.
>
> All Smithsonian systems must display, at the minimum, the System Use Notification (Logon Warning Screen) shown in Appendix C. The System Use Notification must remain on the screen until the user takes explicit actions to log on to the information system.

For publicly accessible systems: (i) the system use information must be available as opposed to displaying the information before granting access; (ii) there should be no references to monitoring, recording, or auditing since privacy accommodations for such systems generally prohibit those activities; (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

We noted that IT-930-02 did not include or make reference to:

- The user is accessing a U.S. Government information system
- System usage may be monitored, recorded, and subject to audit
- Use of the system indicates consent to monitoring and recording

Without displaying adequate warning banners, which all individuals accessing the Institution's general support system are required to agree with, management's ability to enforce penalties for unauthorized activities is diminished.

> Unauthorized computer access is a criminal violation of the Computer Fraud and Abuse Act (18 U.S.C)
>
> System usage limitations are described in Smithsonian directive SD931. All users must read and understand Smithsonian Directive 931, sign a User Agreement, and take the online computer security awareness training annually.
>
> Bypass of this banner implies understanding and acceptance of the policies in SD 931 and agreement to obtain, use or disclose sensitive data only in connection with performance of authorized official duties.
>
> While using Smithsonian computers and networks, you should have no expectation of privacy. Report any violation of these policies to the Smithsonian Computer Security Manager, Bruce Daniels, at (202) 633-6000 or William McGeehan at (202) 633-0632.

Recommendations

We recommend that the CIO:

7. Update IT-930-02 to include language identified by NIST SP 800-53.

8. Update all SInet warning banners to ensure they are consistent and address all language required by NIST SP 800-53.

Session-Locking Controls are Not Implemented

Controls are not adequate to ensure workstations on SInet lock after a period of inactivity. Although we noted the Institution has developed a policy (IT-930-01 *Activating Password-Enabled Screensaver*) requiring users to configure their workstations to activate a password-protected screensaver when the computer has been idle for 10 minutes or less, we noted this policy has not been adequately implemented by users or enforced by the Directors of each museum, research institute, or office. Specifically, our audit identified workstations on SInet that were not configured to activate a password-protected screensaver within the 10 minute required time period.

Additionally, we noted that the Institution's current mixed environment of Windows and Novell prohibits them from effectively pushing down controls over inactivity to the user's workstation. Without adequate controls in place to ensure that idle workstations lock after a period of inactivity, the risk of unauthorized individuals gaining access to an unattended workstation increases.

Recommendations

We recommend the CIO:

9. Enforce Institution policy requiring activation of password-protected screensavers after a period of inactivity not to exceed 10 minutes. For example, OCIO should consider performing periodic random audits of user's workstations to ensure they are properly configured.

10. Where feasible, use Microsoft Active Directory to push screensaver controls down to user's workstations.

Password Controls are Not Enforced

Controls are not adequate to ensure passwords protecting users' SInet accounts comply with Institution policy. Specifically, we determined users' SInet accounts are not being consistently configured to require users to change their password every 90 days.

The SInet system security plan section IA-5 *Authenticator Management* states:

> Where supported by the software, passwords expire after 90 days and cannot be reused for 12 generations.

The Institution has developed a policy that users are required to change their passwords every 90 days, and system administrators are to periodically review their accounts. However, out of 6,188 user accounts and 202 system-related accounts logged into during FY2006 (10/01/05 through 07/20/06), we determined:

- 265, or 4%, of user accounts passwords had not been changed in over 90 days.
- 62, or 31%, of system accounts passwords had not been changed in over 90 days

Through interviews we learned that no assessments are conducted to ensure that administrators periodically review the password controls and make changes in accordance with Institution policy.

Recommendation

11. We recommend that the CIO enforce Institution policy by ensuring SInet implements strong password controls, including having passwords for all accounts change, at a minimum, every 90 days.

Signed Rules of Behavior are Not Retained

Controls are not adequate to ensure signed rules of behavior for all SInet users are on file. Smithsonian Directive (SD) 931, *Use of Computers and Networks*, documents rules of behavior, assignments of responsibility, and penalties for non-compliance. SD 931 states:

The Director, Office of Human Resources, ensures that:

- Computer security awareness training is included in orientation of new employees
- Employees sign user agreements during orientation
- Signed user agreements are retained in the official personnel files of all employees.

The director of each museum, research institute, and office ensures that

- Each user annually completes the online computer security awareness tutorial
- Users who are not Smithsonian employees sign user agreements
- Signed user agreements are retained in unit files.

Our testing of a random sample of 45 SInet users noted that management could not provide signed user agreements for 22 of the 45 employees and contractors tested. Specifically, we noted:

- 22 SInet accounts tested had signed user agreements.
- One current employees' user agreement was signed, but the signature date was after the time of our initial testing.
- One current employees' user agreement could not be provided for review.
- Signed user agreements for 16 contractors with access to SInet could not be provided.
- Five SInet user accounts tested were for employees no longer working at the Smithsonian. According to the Office of Human Resources, files for these employees were purged so no signed user agreements were available for review.

Without signed user agreements, management's ability to hold users accountable for unauthorized or inappropriate activities on SInet decreases. In addition, without effectively communicating expected behaviors to SInet users, management cannot be sure users are not unknowingly performing unauthorized or risky activities on the network.

Recommendations

We recommend that the Director, Office of Human Resources, and the CIO:

12. Work together to determine the best way to comply with Smithsonian policy SD 931, *Use of Computer and Networks,* by retaining signed user agreements in the official personnel files of all employees. Signed agreements should be retained in a format that can be easily retrieved in the future.

We recommend that the CIO:

13. Require existing users of SInet who do not have signed agreements on file to re-sign user agreements.

14. Develop and implement procedures to ensure that the director of each museum, research institute, and office retains signed user agreements for non-Smithsonian personnel working in their units as required by SD 931.

Risk Assessments Do Not Address NIST Requirements

Controls are not adequate to ensure risk assessments performed by the Institution adequately address the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Institution. While OCIO did perform a risk assessment of SInet, this risk assessment did not address specific areas recommended by NIST SP 800-30 *Risk Management Guide for Information Technology Systems*. Specifically, the SInet risk assessment, provided by management, did not include:

- List of threat sources that are a risk to SInet
- List of the motivations or threat actions related to the threat sources
- List of threat sources not tied to vulnerabilities
- Identification of threats from system security testing results (vulnerability scans, penetration testing, and security testing and evaluation)
- Security requirements checklist
- Identification of the likelihood, impact, or risk for each vulnerability
- Risk-level matrix or a description of the risk levels

In addition, we noted the SInet risk assessment did not clearly identify a history of changes to the risk assessment or names of individuals involved in performing the most recent risk assessment. While NIST does not specifically require this information to be included in the risk assessment, this information is important to ensure all changes to the environment under review have been addressed and the right people have been included in the risk assessment process.

Without developing and maintaining a complete risk assessment, it becomes difficult for management to assess and prioritize all potential threats and vulnerabilities.

Recommendations:

We recommend that the CIO:

15. Revise the documented SInet risk assessment to reflect all requirements from NIST SP 800-30.

16. Develop, document, and implement procedures to ensure future risk assessments address all areas identified in NIST SP 800-30.

Wireless Policies and Procedures Need to be Updated

Controls are not adequate to ensure unauthorized or unencrypted wireless networks are not attached to SInet. OCIO has developed and documented a policy and procedures on the use of wireless technologies within the Institution. Technical Note IT-930-TN25, *Wireless Networks and Mobile Devices*, states:

> At this time wireless devices are specifically prohibited from connection to SInet. In extraordinary circumstances and where adequate controls can be demonstrated a waiver may be granted. The waiver must be approved by the Director Office of Information Technology Operations (OITO), and the Smithsonian Computer Security Manager. Implementation guidance will be approved as part of the waiver process. Waivers may be granted for more than one calendar year.

> OCIO will monitor wireless access points and will take action to disconnect any unapproved devices.
>
> The computer security manager will use available tools to monitor Smithsonian computer resources.

However, our review of IT-930-TN25 noted that specific procedures have not been identified or documented for the computer security manager to follow when monitoring Smithsonian computer resources. The Institution's policy does not state how monitoring will occur or how often monitoring should occur.

Without adequate monitoring procedures in place to identify unauthorized wireless networks, management cannot be sure individuals with access to SInet are not creating unauthorized wireless networks. The introduction of unauthorized and in some cases unencrypted wireless networks to an Institution's infrastructure or general support system can greatly increase the risks of unauthorized individuals gaining access to Institution resources. The use of wireless technologies can lessen or eliminate the effectiveness of border security controls such as firewalls and routers by enabling individuals outside the Institution to attach to the wireless network and thus subvert established controls.

Recommendation

17. We recommend that the CIO update current wireless polices and procedures to specifically identify how management will periodically scan for or prohibit the implementation of unauthorized wireless networks.

Summary of Management's Response

The CIO's July 27, 2007, and the OHR Director's July 9, 2007, responses to our draft report generally concurred with our findings and 15 of our 17 recommendations to strengthen the management, operational, and technical controls over the Smithsonian Institution Network. The CIO agrees with our assessment that policies and procedures for the administration and security of SInet have not been consistently applied. The CIO contends that the only viable long-term solution to the decentralized environment is to consolidate IT responsibilities, along with the assignment of the needed staff to the various roles. The Institution's migration to Active Directory also will significantly improve OCIO's ability to implement more stringent security controls.

The CIO stated that remediating identified vulnerabilities and enforcing proper separation of administrative and security functions will require additional resources not currently budgeted for in OCIO. Moreover, management disagreed with our recommendations to ensure that the current SInet risk assessment and future risk assessments be strengthened. OCIO believes that their risk assessment already meets NIST requirements.

Management's planned actions are summarized below:

Recommendation 1. Concur. OCIO will assign the responsibility for periodic review of all SInet system and user accounts to the OCIO Customer Service and Support Division by December 30, 2007.

Recommendation 2. Concur. OCIO agreed to develop policy and procedures for maintaining SInet access request forms in a format which can be used for future account reviews by December 30, 2007.

Recommendation 3. Concur. OCIO will develop a policy to centralize administration of SInet accounts by January 31, 2008, for all SInet users within Active Directory. This Institution-wide policy will include guidance for OIG accounts.

Recommendation 4. Concur. OCIO will enforce policies and procedures for pushing vendor security patches and security hot-fixes and has provided a target completion date of February 28, 2008.

Recommendation 5. Concur. OCIO agreed that the process for scanning for vulnerabilities and ensuring that weaknesses are mitigated needs improvement. OCIO agreed to perform, by October 30, 2007, a SANs - top 20 – non-intrusive vulnerability scan against the identified IP addresses. OCIO agreed to remediate identified vulnerabilities, but indicated that current staffing levels and the decentralized nature of the Institution make it difficult to assign responsibility for remediation.

Recommendation 6. Concur. While OCIO agreed that separation of duties is desirable, due to lack of resources and funding they are not currently able to implement this recommendation. OCIO will request the establishment of a security position in the Office of Information Technology Operations to assume responsibility for SInet security by early 2008 for inclusion in the FY 2010 budget. In lieu of not securing the funding, OCIO will consider additional automation tools to facilitate the monitoring of security controls and activities.

Recommendations 7 and 8. Concur. OCIO indicated that it will update IT-930-02 to include warning banner language identified in NIST SP 800-53 and implement new banners for SInet Active Directory and Novell logins by July 30, 2007.

Recommendations 9 and 10. Concur. OCIO will implement, by November 30, 2007, a group policy in Active Directory requiring the activation of password-protected screensavers.

Recommendation 11. Concur. Once all SI units move to Active Directory, no later than November 30, 2007, OCIO will improve enforcement of SI password policy as outlined in SD 931.

Recommendation 12. OHR and OCIO concur. OHR believes this recommendation to be unnecessary since there appears to be a single employee file identified during the audit that was missing the signed user agreement. This file was for an employee who was subject to a staff reduction and the user agreement had likely been purged, in accordance with Office of Personnel Management regulations. The Associate Director, OHR, conducted additional testing of 50 employees to ensure that signed user agreements were contained in the personnel folders and without exception all folders were compliant.

Recommendations 13 and 14. Concur. Effective June 2007, OCIO has deployed an electronic signature procedure whereby user agreements will be signed annually as part of the Computer Security Awareness Training process. To ensure that this process is operating as intended, covering all employees, contractors, and other users with access to SInet, OCIO proposed a target completion date of September 30, 2008.

Recommendations 15 and 16. Non-concur. OCIO believes the risk assessment documentation adequately reflects the intent and overall guidance of NIST SP 800-30.

Recommendation 17. Concur. By September 30, 2007, OCIO will update existing policies to reflect management procedures for tracking down unauthorized wireless access points including investigating devices identified through OCIO network scans.

We include the full text of management's response in the Appendix to this report.

Office of the Inspector General Comments

Management's planned actions for recommendations 1 through 14 and 17 are responsive to the intent of our recommendations and we consider them resolved. For recommendation 3, we agree with OCIO's planned actions to centralize administration of SInet accounts for all SInet users within OCIO. We understand that the inclusion of the OIG in this policy was not meant to suggest that OCIO would be administering OIG accounts but merely providing guidance on administration of forms. For reasons of independence, the OIG will administer its own accounts.

For recommendation 7, we verified that OCIO updated IT-930-02 to include warning banner language identified in NIST SP 800-53. Therefore, we will close this recommendation. We also held numerous discussions with OHR on recommendation 12. Based on OHR's assurances that it will continue to require new employees to sign user agreements during orientation and file them in the personnel folder and OCIO's procedure that it implemented in June 2007 to have employees electronically sign user agreements annually when taking security awareness training, we consider this recommendation closed as well.

In evaluating management's response to this report, we held several discussions with the IT Security Director in an effort to clarify and resolve areas of disagreement. The only recommendations we could not ultimately reach resolution on are recommendations 15 and 16 on SInet's risk assessment. While OCIO indicates that it used the sample risk assessment in Appendix C of NIST SP 800-30, we believe that had OCIO followed the process prescribed in the body of NIST SP 800-30, they would have identified several more significant risks. For example, the SInet risk assessment does not consider the following:

- The Institution's highly decentralized environment and numerous physical remote locations result in a variety of personnel, remote access, networking and physical security risks.
- Temporary network users (such as researchers or summer interns).
- The Institution is a high-profile organization making it an attractive target by outsiders.
- The potential for personally identifiable information (relating to federal or non-federal employees, donors, and members of the public) being transmitted through the general support system.

We, as well as Cotton & Co., continue to believe that the SInet risk assessment does not adequately address the NIST requirements detailed earlier in this report. OCIO's interpretation of these missing items is inconsistent with how NIST describes each of them. For example, NIST SP 800-30 describes threat sources as who or what exploited the vulnerability and the threat action is the specific discussion of how the vulnerability can be exploited. In addition, the guidance also discusses the motivation of the threat source. While OCIO has listed threats, it has not identified threat sources, actions, or motivations.

Despite our disagreement on this issue, OCIO, our office and Cotton & Co. have committed to meet to work on the development of a model Risk Assessment plan. We believe the development and implementation of such a plan would benefit all Smithsonian information systems and will satisfy the intent of the recommendations.

We appreciate the courtesy and cooperation of Smithsonian representatives during this audit.

Appendix – Management Response

Smithsonian Institution Memo

Date July 27, 2007

To Sprightley Ryan, Inspector General

cc Sheila Burke, Deputy Secretary and Chief Operating Officer

From Ann Speyer, Chief Information Officer

Subject Response to the Draft Report, Office of the Inspector General Audit A-06-07, On the Fiscal Year 2006 Smithsonian Institution Network (SInet)

Thank you for the opportunity to comment on the draft audit report on the Smithsonian Institution Network (SInet).

The report states that: "Our audit of the Institution's general support system noted that the Institution operates in a decentralized environment where responsibility for both performing functions and enforcing IT controls has been assigned to the same individuals. Responsibility for administration and security of SInet has not been centralized under OCIO and, as a result, IT security policies and procedures documented by OCIO have not been consistently implemented or followed."

Based on the above reference we believe the only viable long term solution to this problem is a consolidation of IT responsibilities centrally, along with the assignment of the needed staff to the various roles. As such the migration of computers to a single authentication environment (active directory) – AD will also significantly improve our ability to implement more stringent security controls.

As stated the attachment references each issue presented in the audit report and our response in the order it was presented. If you would like to discuss our response or have any questions please contact me at 202-633-1688 or Bruce Daniels, Smithsonian Computer Security Manager, at 202-633-6000.

Attachment

Appendix – Management Response (continued)

Attachment

Issue 1: **NETWORK ACCOUNT ADMINISTRATION PROCEDURES ARE WEAK**

"Controls over the administration of SInet accounts are not adequate. System administrators are not managing SInet accounts in accordance with Institution or NIST policy. Responsibility for adding, deleting, and maintaining SInet accounts has been assigned to various administrators across the Institution."

Response: OCIO agrees with the finding and is working to implement the OIG's recommendation.

Issue 1 Recommendations

Recommendation 1: Assign responsibility to someone within OCIO for periodically reviewing all SInet system and user accounts to determine whether they are still necessary. For example, periodic reviews should detect active accounts with no activity in the last 180 days or accounts associated with individuals who have recently left the Institution.

Comment: Concur. The only account management conducted by the Network Infrastructure group is Active Directory accounts. OCIO will assign the responsibility for periodic review of all SInet system and user accounts to the OCIO Customer Service and Support Division who will work with reports generated by the Data Center Operations & Network Server Administration Division of the Office of Information Technology Operations.

Target Completion Date: December 30, 2007

Recommendation 2: Develop a policy and procedures for maintaining SInet access request forms in a format which system or security administrators will be able to use for future reviews of network accounts.

Comment: Concur. The only account management conducted by the Network Infrastructure group is Active Directory accounts. OCIO agrees to develop a policy and procedures for maintaining SInet access request forms in a format which can be used for future account reviews

Target Completion Date: December 30, 2007

2

Appendix – Management Response (continued)

Recommendation 3: Centralize administration of SInet accounts for all SInet users within OCIO with the exception of the Office of the Inspector General

Comment: Concur. OCIO will develop a policy for all SInet user accounts within Active Directory. SI-wide policy will include OIG accounts.

Target Completion Date: January 31, 2008

Issue 2: **TECHNICAL CONTROLS OVER SINET NEED TO BE STRENGHTENED**

Controls need to be strengthened to ensure that significant technical weaknesses do not exist on SInet.

Many of these weaknesses related to default configurations not being changed when systems were installed or patches and hot fixes not being implemented in a timely manner.

Installation delays of vendor patches and fixes to the network operating system for known vulnerabilities exposes the Institution's network to an increased risk of successful hacker attacks. It also increases the potential for network sabotage, theft of the organization's sensitive financial and personal data, and destruction and corruption of databases.

Issue 2 Recommendations

Recommendation 4: Enforce policies and procedures for ensuring that vendor patches and security hot-fixes are installed in a timely manner.

Response: Concur. OCIO is currently enforcing policies and has procedures for pushing vendor security patches

Target Completion Date: February 28, 2008

Recommendation 5: Review results of our technical testing (provided during earlier meetings) to ensure weaknesses identified have been addressed by management or identified in OCIO scans. In addition, ensure critical weaknesses such as the ones identified in the SANS Top-20 are addressed first and lower-level risk items addressed later.

Response: Concur. OCIO is routinely scanning for vulnerabilities and working to remediate these. OCIO agrees that this process can be improved by the completion of the move to Active Directory and by the addition of staff. Current staffing levels and the

3

Appendix – Management Response (continued)

decentralized nature of the Smithsonian make it difficult to assign responsibility for remediation. We question the value of comparing old scans to new scans. It seems better to remediate identified vulnerabilities than to attempt to reconcile two scan versions. OCIO agrees to perform a Foundstone SANs FBI - top 20 – non-intrusive vulnerability scan - against the identified IP addresses.

Target Completion Date: October 30, 2007

Issue 3: **DUTIES ARE NOT ADEQUATELY SEGREGATED**

"Controls are not adequate to ensure sensitive activities within SInet have been adequately segregated.

"We determined management has not enforced proper separation of administrative and security functions. Our audit noted individuals responsible for administration of SInet user accounts in many cases are also responsible for the review of system audit logs. Security best practices do not allow the same individual both to set up new users and review audit logs. Without separation of administration and security functions, management cannot ensure individuals with high-level or sensitive access to the system are not performing unauthorized activities."

Response: We agree with the findings. OCIO is working to implement the OIG's recommendation. We agree that separation of duties is desirable, however due to lack of resources and funding we are not able to currently implement this recommendation.

Issue 3 Recommendations

We recommend that the CIO:

Recommendation 6: Enforce separation of duty controls noted in the SInet system security plan and specifically segregate system administration roles from security roles.

Comment: Partial-Concur. OCIO does not have existing staff resources to allow this currently. OCIO will request the establishment of a security position within OITO – this position would assume responsibility for SInet security plans.

Target Completion Date: TBD

Issue 4: WARNING BANNERS ARE NOT CONSISTENTENTLY APPLIED

"Controls are not adequate to ensure SInet warning banners include language required by the Institution and NIST"

4

Appendix – Management Response (continued)

Response: OCIO agrees that the warning banners could be improved and be more specific in regard to monitoring.

Issue 4 Recommendations

We recommend that the CIO:

Recommendation 7: Update IT-930-02 to include language identified by NIST SP 800-53

Comment: Concur. OCIO has updated warning banners to include language identified in NIST SP 800-53.

Target Completion Date: July 30, 2007

Recommendation 8: Update all SInet warning banners to ensure they are consistent and address all language required by NIST SP 800-53.

Comment: Concur. OCIO has implemented the new banners described above for SInet Active Directory and Novell logins.

Target Completion Date: July 30, 2007

Issue 5: SESSION-LOCKING CONTROLS ARE NOT IMPLEMENTED

"Controls are not adequate to ensure workstations on SInet lock after a period of inactivity."

Response: This has been on the blueprint for OCIO since we began migration to Active Directory. Unfortunately until all SI units are in Active Directory this is problematic. We will implement this once movement to Active Directory is completed

Issue 5 Recommendations

We recommend that the CIO:

Recommendation 9: Enforce Institution policy requiring activation of password-protected screensavers after a period of inactivity not to exceed 10 minutes. For example, OCIO should consider performing periodic random audits of user's workstations to ensure they are properly configured.

5

Appendix – Management Response (continued)

Comment: Concur. OCIO will implement a group policy In Active Directory requiring the activation of password-protected screensavers once completion to Active Directory is completed.

Target Completion Date: November 30, 2007

Recommendation 10: Where feasible, use Microsoft Active Directory to push screensaver controls down to user's workstations.

Comment: Concur. As above - OCIO will implement a group policy In Active Directory requiring the activation of password-protected screensavers once completion to Active Directory is completed

Target Completion Date: November 30, 2007

Issue 6: PASSWORD CONTROLS ARE NOT ENFORCED

"Controls are not adequate to ensure workstations on SInet lock after a period of inactivity."

Response: This also has been on the blueprint for OCIO since we began movement to Active Directory. Unfortunately until all SI units are in Active Directory this is problematic. We will implement this once movement to Active Directory is completed

Issue 6 Recommendations

We recommend that the CIO:

Recommendation 11: We recommend that the CIO enforce Institution policy by ensuring SInet implements strong password controls, including having passwords for all accounts change, at a minimum, every 90 days.

Comment: Concur. Unfortunately until all SI units are in Active Directory this is problematic. OCIO will enable improved enforcement of SI password policy as outlined in SD 931 after all units have been moved to Active Directory. OCIO will use group policies to enforce password controls for all accounts in Active Directory,

Target Completion Date: November 30, 2007

Issue 7: SIGNED RULES OF BEHAVIOR ARE NOT RETAINED

"Controls are not adequate to ensure signed rules of behavior for all SInet users are on file."

Appendix – Management Response (continued)

Response: OCIO believes that signed rules of behavior exist for all staff. All new employees are required to sign these forms and the forms are managed by OHR. Experience has shown that units are good about making sure that user agreements are signed. Unfortunately the current processes are not conducive to the easy retrieval of the forms. Even OCIO has a difficult time with forms that are faxed to it because the forms are associated with the individual requesting the account and not the individual receiving the accounts and signing the user agreement. We note that the auditors did not request forms from the correct individuals in many cases. OHR maintains forms only for employees

We believe that OHR should continue to get signed user agreement at employee orientation and should maintain these agreements. We feel that OCIO should supplement this with a central account policy that allows us to address all accounts. We also feel that users should electronically resign user agreements annually.

Issue 7 Recommendations

To Director, Office of Human Resources and the CIO

Recommendation 12: Work together to determine the best way to comply with Smithsonian policy SD 931, *Use of Computer and Networks*, by retaining signed user agreements in the official personnel files of all employees. Signed agreements should be retained in a format that can be easily retrieved in the future.

Comment: Concur. OCIO believes that SI is currently compliant with SI policy but concedes that retrieval of forms is probably difficult. OCIO will work with OHR to see if a more effective set of procedures can be developed.

Target Completion Date: TBD

Recommendation 13: Require existing users of SInet who do not have signed agreements on file to re-sign user agreements.

Comment: Concur. OCIO proposes having users electronically sign the user agreements annually as part of the Computer Security Awareness Training process. This procedure was made effective in June, 2007.

Target Completion Date: September 30, 2008

Recommendation 14: Develop and implement procedures to ensure that the director of each museum, research institute, and office retains signed user agreements for non-Smithsonian personnel as required by SD 931.

Comment: Concur. OCIO has deployed an electronic signature procedure for having

7

Appendix – Management Response (continued)

users sign agreements. Users will electronically sign the user agreements annually as part of the Computer Security Awareness Training process. This procedure was made effective in June, 2007.

Target Completion Date: September 30, 2008

Issue 8: RISK ASSESSMENTS DO NOT ADDRESS NIST REQUIREMENTS

"Controls are not adequate to ensure risk assessments performed by the Institution adequately address the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Institution. While OCIO did perform a risk assessment of SInet, this risk assessment did not address specific areas recommended by NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. ."

Based on discussion with the IG where OCIO pointed out that several items listed in the original version were in fact present in the Risk assessment OCIO was advised that the IG wanted this changed to read:
RISK ASSESSMENTS DO NOT ADDRESS NIST REQUIREMENTS

Controls are not adequate to ensure risk assessments performed by the Institution adequately address the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Institution. While OCIO did perform a risk assessment of SInet, this risk assessment did not address specific areas recommended by NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems. Specifically, the SInet risk assessment, provided by management, did not include:

* List of threat sources that are a risk to SInet
* List of the motivations or threat actions related to the threat sources
* List of threat sources not tied to vulnerabilities
* Identification of threats from system security testing results (vulnerability scans, penetration testing, and security testing and evaluation)
* Security requirements checklist
* Identification of the likelihood, impact, or risk for each vulnerability
* Risk-level matrix or a description of the risk levels

In addition, we noted the SInet risk assessment did not clearly include the history of changes to the risk assessment or names of individuals involved in performing the most recent risk assessment. While NIST does not specifically require this information to be included in the risk assessment, this information is important to ensure all changes to the environment under review have been addressed and the right people have been included in the risk assessment process.

8

Appendix – Management Response (continued)

Without developing and maintaining a complete risk assessment, it becomes difficult for management to assess and prioritize all potential threats and vulnerabilities.

Response: OCIO does not concur with this finding. We believe the risk assessment documentation adequately reflects the intent and overall guidance of NIST SP 800-30.

As an example the table (Table I) presented below provides evidence that we have followed the guidance as stated.

* List of threat sources that are a risk to SInet

The table identifies below includes threats.

Threat/Vulnerability	Likelihood	Impact	Risk	Safeguard
1. Physical Security				
Unauthorized access to network cables	Medium	Medium	Medium	
Unauthorized access to wiring closets	Low	Medium	Medium	Where possible continue Installing locks or build lockable closets
Unauthorized access to A&I or Victor Bldg computer rooms	Low	High	Medium	In place: Require everyone who enters these rooms to wear their badge, and escort visitors.
2. Personnel Security				
Background checks not done for contractors	Low	High	Medium	Require NAC checks for all contractors who maintain SInet

* List of the motivations or threat actions related to the threat sources

While motivations are not discussed the vulnerabilities identified in the above table were meant to represent threat actions.

* List of threat sources not tied to vulnerabilities

From the above table the threat sources have been identified in broad categories. Thirteen of these are identified in the table present in the Risk Assessment. They are: Physical Security; Personnel Security; Logical Access Controls; Environmental; Natural Disasters; Software Controls; Communications; Media Controls; Documentation; User Training; Audit Trails; Separation of Duties, and Hardware failure ,

9

Appendix – Management Response (continued)

* Identification of threats from system security testing results (vulnerability scans, penetration testing, and security testing and
evaluation)

As stated in the Risk Assessment document

The Risk Assessment reflects lessons learned during the course of several penetration tests conducted in FY 2005. These tests were against the network infrastructure in general and one against the VOIP component of the infrastructure.

- Security requirements checklist

A checklist of security requirements (other than those present in the System Security Plan – are identified as part of the previously referenced table (Safeguard)). In addition the Summary section of the document itemized 13 separate actions to be undertaken to mitigate identified risks.

* Identification of the likelihood, impact, or risk for each vulnerability

The likelihood, impact, or risk for each vulnerability is identified under the columns Likelihood / Impact / Risk in the table identified above

- Risk-level matrix or a description of the risk levels

We contend that the Risk levels are identified in the table previously identified under the column risk. Risk levels are labeled as low, moderate or high using the criteria present in NIST SP 800-30 (pg. 25)

- History of changes is addressed. However the name of the individual updating the Risk Assessment is not present.

As pointed out this is not a NIST SP 800-30 requirement.

OCIO believes that the Risk Assessment as it exists fulfills the purpose of a Risk Assessment and meets the basic requirements identified in NIST SP 800-30.

OCIO is willing to meet with the IG's office to work on the development of a model Risk Assessment plan.

Issue 8 Recommendations

We recommend that the CIO:

Recommendation 15: Revise the documented SInet risk assessment to reflect all requirements from NIST SP 800-30.

Comment:. Non-concur. OCIO believes that the current Risk Assessment meets the basic requirements of SP 800-30. We have addressed each of the identified deficiencies above.

10

Appendix – Management Response (continued)

Target Completion Date: Not Applicable

Recommendation 16: Develop, document, and implement procedures to ensure future risk assessments address all areas identified in NIST SP 800-30.

Comment: Non-concur. OCIO believes that the current Risk Assessment meets the basic requirements of SP 800-30. We have addressed each of the identified deficiencies above.

Target Completion Date. Not Applicable

Issue 9: WIRELESS POLICIES AND PROCEDURES NEED TO BE UPDATED

"Controls are not adequate to ensure unauthorized or unencrypted wireless networks are not attached to SInet."

Response: OCIO prohibits the use of wireless access points with a few exceptions most of which are in heavily enclosed spaces.

Issue 9 Recommendations

We recommend that the CIO:

Recommendation 17: We recommend that the CIO update current wireless polices and procedures to specifically identify how management will periodically scan for or prohibit the implementation of unauthorized wireless networks.

Comment: Concur. OCIO has for the past 6 months been aggressive in trying to track down unauthorized wireless access points. As a product of the periodic network scans we investigate devices that may be wireless. Also we investigate ip addresses that show up in our Network Behavior Analyzer which may have been generated as the result of a wireless AP performing DHCP. OCIO will update existing policies to reflect these management procedures.

Target Completion Date: September 30, 2007

11

Appendix – Management Response (continued)

Smithsonian Institution Memo

Office of Human Resources

Date: July 9, 2007

To: A. Sprightley Ryan
Inspector General

cc: Ann Speyer
Chief Information Officer

From: James D. Douglas, Director
Office of Human Resources

Subject: Review of Draft Report A-06-07, Fiscal Year 2006 Smithsonian Institution (SInet) Audit

Thank you for the opportunity to review the draft Inspector General report A-06-07, "Fiscal Year 2006 Smithsonian Institution Network (SInet) Audit."

There is one recommendation addressed jointly to the Office of Human Resources (OHR) and the Office of the Chief Information Officer (OCIO). Recommendation #12 asks OHR and OCIO work together to determine the best way to comply with existing Smithsonian policy by retaining signed user agreements for employees in official personnel folders, and that they should be retained in an easily-retrievable format.

We agree that user agreements for employees should be retained in the Institution's official personnel folders. Since those files are hard copy only, all documents retained in hard copy files are, by definition, in hard copy format.

This recommendation, however, appears unnecessary. The initial report from the contractor made no distinction between employees and non-employees, stating that the signed agreements were not in employee files. OHR contacted and worked with your staff to go through the list name by name, and those on the list who were active employees were pulled. Of those sampled, only one did not have a user agreement on file, and that record was for an employee who had previously been subject to a staff reduction, and it is likely that the user agreement was purged as part of the normal file processing when an employee separates

In terms of separated employees, we wanted to provide some background information. Office of Personnel Management (OPM) regulations govern what may or may not be retained in official personnel folders, and documents are referred to as long-term or temporary documents. According to OPM's Guide to Personnel Record-Keeping, "the right side of the personnel folder is reserved for long-term documents. Only documents authorized by the Office of Personnel Management may be placed on the right side of the folder." The Smithsonian's user agreements

Appendix – Management Response (continued)

are not authorized by OPM as long-term documents, and thus they are considered temporary. When an employee separates, only the record of leave data, any documentation of indebtedness, and performance records are temporary documents that are kept in the file. All other temporary documents are removed in accordance with OPM regulations. As signed user agreements are temporary, and OPM requires the Institution to remove them when an employee separates, it would violate Federal regulations if we were to keep the user agreements in the official personnel files.

OHR's current process ensures that all new employees sign the computer user agreement, and the employees conducting orientation are given a checklist of documents that must be received from the employee at the end of the orientation session. The computer user agreement is on that checklist. Those documents, collected at orientation, are the first set of documents to be placed in a new employee's folder.

The sampling of current employees shows that they have the user agreements in the file, with the exception of one. We feel that the exception is one stemming from a staff reduction and does not represent a systematic problem.

Given this information, we do not feel that this is a necessary recommendation, and we recommend that it be eliminated.