**Smithsonian Institution**
**Office of the Inspector General**

# In Brief

## Smithsonian Institution Network Infrastructure (SINet)
**Report Number A-09-01, September 30, 2009**

### Why We Did This Audit

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 system. As part of that assessment, FISMA requires a review of a subset of information systems. This report covers one such system, the Smithsonian Institution Network Infrastructure (SINet), and the evaluation of associated management, operational, and technical security controls.

### What We Recommended

We made two recommendations to strengthen controls over the SINet general support system. We recommended that the CIO direct the CISO to improve the effectiveness of vulnerability scans by addressing the limitations of the scanner in use. We also recommended that the CIO direct two systems owners to remediate the identified vulnerabilities in accordance with CIO procedures.

Management concurred with our findings and recommendations and has planned actions that will resolve all our recommendations.

### What We Found

SINet provides network services to more than 11,000 end-users as well as access to administrative and program applications and databases throughout the organization. SINet spans a large geographical area, including many buildings and museums in the Washington DC area, the Smithsonian datacenter, research and museums in several states, and facilities in Panama.

Overall, we determined that operational, management, and technical controls were substantially in place and operating effectively. While management has complied with the majority of Institution, OMB, and NIST requirements, we did identify two areas where management needs to implement improvements. Specifically, we found that:

- The Office of Chief Information Officer performs scans of parts of the network throughout the year using a vulnerability scanner. However, this scanner did not identify vulnerabilities identified by the auditors using different tools. Management confirmed that the additional higher-risk vulnerabilities existed.

- As a result of our identification of additional vulnerabilities, management needed to apply patches to the devices affected.

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 2009
# INDEPENDENT PERFORMANCE AUDIT OF SINET

## 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 2009**
**INDEPENDENT PERFORMANCE AUDIT OF SINET**

**SMITHSONIAN INSTITUTION**
**OFFICE OF THE INSPECTOR GENERAL**

## PURPOSE

Cotton & Company LLP conducted an independent performance audit of the Smithsonian Institution's (Institution) security management programs and practices to determine the effectiveness of management, operational, and technical security controls over the Smithsonian Institution Network (SINet).

## BACKGROUND

The E-Government Act of 2002 (Public Law 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 Institution is not subject to the E-Government Act of 2002, the Institution has elected to comply with FISMA because it is consistent with and advances the Institution's mission and strategic goals.

FISMA outlines federal information security requirements, including an annual independent assessment by the Institution's Inspector General. This report provides details of the performance audit of SINet management, operational, and technical security controls and supports the Smithsonian Institution Office of the Inspector General's (OIG) annual FISMA evaluation of information security controls implemented by the Institution based on work performed by Cotton & Company.

FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) specify 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 by FIPS, through the use of the security controls set forth in NIST Special Publication (SP) 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*.

  The use of security controls from NIST SP 800-53, 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. They also offer the needed flexibility to tailor controls based on specific organizational policy and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk to the organization's operations and assets.

- **Annual System Security Control Assessments**. NIST's 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.

On behalf of the OIG, Cotton & Company performed an independent audit of one of the Smithsonian's general support systems (GSS), SINet. We conducted this audit in accordance with *Government Auditing Standards*, 2007 Revision, as amended, promulgated by the Comptroller General of the United States. These 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 audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on audit objectives. This report is intended to meet the objectives described below and should not be used for other purposes.

SINet provides network services to more than 11,000 end-users as well as access to administrative and program applications and databases throughout the organization. SINet spans a large geographical area, including many buildings/museums in the Washington, DC area, the Smithsonian datacenter, and research locations and other museums in several other states, as well as Panama. SINet consists primarily of networking hardware (such as routers, switches, intrusion detection systems [IDS], and firewalls) and servers providing common services (such as file servers, mail servers, and domain name servers) for major and minor applications. For Institution sites that are remote to the Washington, DC Mall area, the Institution uses leased point-to-point high-speed data service lines from several local carriers. These lines do not traverse the public internet. Remote users are also able to securely access the network and its resources via a virtual private network (VPN). All external access is routed through the main Smithsonian datacenter, where the primary firewalls and IDSs are located.

## OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this independent audit were to evaluate and report on management's identification, documentation, and implementation of the following management, operational, and technical security controls required by NIST SP 800-53 Revision 2:

- RA-5 Vulnerability Scanning
  - Documented policies and procedures for vulnerability scanning
  - Process/methodology for scanning
  - Identify responsive hosts and information about them
  - Identification of vulnerabilities/weaknesses on hosts
  - Determination of patches on system through weakness identification
  - Penetration testing to exploit weaknesses discovered
  - Review of weaknesses identified

- AC-18 Wireless Access Restrictions
  - Policies and procedures for wireless
  - Identification of wireless devices and infrastructure
  - Use of encryption, specifically, WiFi Protected Access (WPA) or WPA2 standards instead of the older, more vulnerable Wired Equivalent Privacy (WEP) standard
  - Wardriving to identify wireless access points
  - Wireless penetration testing

- SC-7 Boundary Protection
  - External vulnerability scanning and penetration testing

- IR-5 Incident Monitoring
  - Assurance that Smithsonian was able to see scanning and penetration attempts

Three high-risk areas of the wired network were selected for testing. In addition, we also reviewed selected wireless networks due to the inherent higher risks.

To accomplish these objectives, we performed detailed audit procedures over selected controls using technical testing methodologies. We performed the following testing to determine the effectiveness of these controls:

- Internal vulnerability scanning on the three areas using the Nessus vulnerability scanner, a widely used tool to assess weaknesses across a multitude of operating systems, databases, and networking hardware
- Penetration testing on two of the areas selected using exploits associated with discovered vulnerabilities
- External vulnerability scanning using Nessus
- Wireless discovery and penetration using the Kismet wireless identification tool, aircrack-ng, airodump-ng, and airmon-ng; tools used to discover wireless networks, determine the level of security associated with the networks, and exploit weaknesses in the network security

## RESULTS

Controls over the SINet areas we reviewed were substantially in place and operating effectively. Management complied with the majority of NIST, OMB, and Institution requirements for safeguarding sensitive areas of the SINet. During external vulnerability scanning, Institution monitoring utilities successfully identified and blocked further attempts to obtain information on vulnerabilities. In addition, during wireless reviews, we noted no instances where Institution based wireless access points were not using encryption or were using weak WEP encryption. We were also unable to successfully access any of these wireless networks during testing. We did not identify any weaknesses related to the use of wireless technologies during our audit.

We did, however, identify areas where unnecessary risks existed and improvements were needed. During vulnerability scans of SINet, we discovered vulnerabilities in two areas of the network we reviewed. Specifically, we noted:

- Area 3 of the network was vulnerable to a total of 12 critical- and high-risk vulnerabilities, including two unique critical- and two unique high-risk vulnerabilities. These vulnerabilities unnecessarily reduced the security posture of seven devices increasing the risks from unauthorized access and disclosure as well as denial of service attacks. Management confirmed that all critical- and high-risk vulnerabilities identified in this area were actual vulnerabilities. We followed up with management on moderate risks identified in this area but were not able to obtain verification from management that these were in fact vulnerabilities. Specific details of our scanning, including all low, moderate, and high vulnerabilities identified, were provided to management for their review and remediation.

- We identified a total of 8 high risk vulnerabilities, including four unique high-risk vulnerabilities, in area 1. These vulnerabilities unnecessarily reduced the security posture of three devices, increasing the risk of unauthorized access and disclosure as well as denial of service attacks. During penetration testing, we attempted to exploit these weaknesses and gain access to vulnerable systems. We were unable to exploit these vulnerabilities partly because our rules of engagement stated we would not attempt to exploit vulnerabilities that could have a negative impact on production devices. We provided the detailed results from our scans to management.

The Office of the Chief Information Officer (OCIO) performs scans of parts of the network throughout the year using a vulnerability scanner. This includes annual scans of each major application, as well as parts of the GSS not included in major applications themselves. However, this scanner did not identify the vulnerabilities we identified using different tools. RA-5, *Vulnerability Scanning*, requires that appropriate scanning tools are used to identify significant new vulnerabilities. Although mitigating factors, such as firewalls and intrusion detection systems, can reduce the amount of risk to the financial segments where these vulnerabilities were identified, vulnerabilities in these systems still present a risk of unauthorized access to data within systems from both internal and external sources.

**Recommendations**

We recommend that the CIO:

1. Direct the Chief Information Security Officer (CISO) to improve effectiveness of vulnerability scans by addressing the limitations of the scanner in use.
2. Direct the Infrastructure, Enterprise Resource Planning (ERP), and Facility Center System owners to remediate identified vulnerabilities in accordance with CIO procedures.

Smithsonian Institution
Office of the Chief Information Officer

**Date:** September 23, 2009

**To:** A. Sprightley Ryan, Inspector General

**CC:** Alison McNally, Under Secretary for Administration and Finance
George Vandyke, Director OCIO Office of Information Technology Operations
Deron Burba, Director OCIO Office of Modernization
Bruce Daniels, Director of IT Security
Joseph Johnston, Manager Network Management Division
Michelle Gooch, IT Manager Facilities Management System
Jeffrey Shearer, OIG Supervisory Auditor

**From:** Ann Speyer, Chief Information Officer

**Subject:** Response to OIG Draft Audit Report A-09-01, Smithsonian Institution IT Infrastructure (SINet)

Thank you for the opportunity to comment on the FY2009 draft audit report on the Smithsonian Institution IT Infrastructure (SINet).

My office appreciates your acknowledgement in the report that controls over the SInet areas reviewed in the audit were substantially in place and operating effectively. The draft report provided (2) two recommendations and the Office of the CIO concurs with each.

The attachment identifies four (4) Plan of Actions and Milestones (POA&M) which outlines our remediation actions for the two finding. If the OIG does not believe that the projected actions and evidence will be sufficient for closure, please let us know so we can adjust our plan.

Please direct any questions or feedback you may have on our plans to George Vandyke (vandykeg@si.edu 202-633-2716) and Bruce Daniels (Danielsb@si.edu 202-633-6000).

Attachment

P.O. Box 37012
MRC 1010
Washington DC 20013-7012
Phone: 202.3633.1688

*The audit correctly notes that the Institution is not subject to the E-Government Act of 2002 and the OMB guidelines implementing that Act. However, the report goes on to assess the Institution's "compliance" with the Act and OMB guidance and evaluate deficiencies as if the Act and guidelines were applicable. To the extent that the act and OMB guidance reflect best practices, are reasonable in the context of the Smithsonian Institution, and are not in conflict with the Institution's own statutory obligations ("the increase and diffusion of knowledge"), it is the Institution's practice to secure its information consistent with the provisions of the Act and OMB guidance.*

***OIG Recommendation 1 – Direct the CISO to improve the effectiveness of vulnerability scans by addressing the limitations of the existing scanner.***

**Concur.** An SINet POA&M was opened to address this OCIO program recommendation. The POC is identified as Bruce Daniels. **Scheduled Completion Date: 16 December 2009.**

a. The OCIO has licensed an additional industry scanner and will integrate support for this scanner in order to complement existing SI enterprise scan capabilities. Milestone 1 – Completed 21 August 2009.
b. The OCIO opened CCB Heat ticket 538259 to allow the OCIO's new scanner to test for SINet vulnerabilities. Milestone 1 – Completed 02 September 2009
c. The OCIO has opened a heat ticket with out existing scanning vendor to better understand why CVE issues were missed by the scanner. Milestone 3 – Target 16 November 2009.

***OIG Recommendation 2 – Direct the Infrastructure, ERP and Facility Center System owners to remediate identified vulnerabilities in accordance with CIO procedures.***

**Concur.** The following three (3) System POA&Ms will be opened to close out this recommendation.

#1. An SINet Heat Ticket was opened for all High vulnerabilities. An SINet POA&M was opened to address the vulnerability. The System POC is identified as: George Vandyke
**Scheduled Completion Date: 15 April 2010**

a. Heat Tickets 539673 opened. Remediation completed. Heat ticket closed. Milestone 1 – Completed 21 September 2009
b. Scan results are available for OIG review.
c. A SINet POA&M was opened. Milestone 2 - Completed 23 September 2009
d. SI Net weakness remediation. Milestone 3 – Target 15 February 2010.
e. Evidence of clean scan results or documented acceptance of risk. Milestone 4 – Target 15 March 2010

#2. No ERP System Heat Tickets were opened. The ERP IT System Sponsor immediately fixed the critical vulnerability No POA&M required. **Closed**

P.O. Box 37012
MRC 1010
Washington DC 20013-7012
Phone: 202.3633.1688

a. ERP Server moved to ERP development zone with new IP address. No Heat Ticket opened. Milestone 1 – Completed 22 September 2009
b. Evidence of a vulnerability scan results available for OIG Review. Milestone 2 – Completed 23 September 2009

#3. A Facility Management System (FMS) Heat Ticket was opened for the identified high vulnerabilities. An FMS POA&M with corresponding heat tickets was identified to address remediation. The System POC is identified as Cyrus Razavi, razavic@si.edu, 202-633-6358.
**Scheduled Completion Date: 16 November 2009**

a. Heat Ticket 538664 was opened for the high vulnerability. Milestone 1 – Completed September 2009
b. An FMS POA&M was opened. Milestone 2 – Completed 23 September 2009.
c. Evidence of a clean vulnerability scan or documented acceptance of risk. Milestone 3 – Target 15 October 2009

P.O. Box 37012
MRC 1010
Washington DC 20013-7012
Phone: 202.3633.1688

## OFFICE OF THE INSPECTOR GENERAL COMMENTS

**Recommendation 1: Closed.** The OCIO has improved the effectiveness of vulnerability scans by acquiring and implementing a second vulnerability scanner and consulted with the vendor of the existing scanner to determine why vulnerabilities were not identified.

**Recommendation 2: Open.** We noted that OCIO has developed a course of action for ensuring that identified weaknesses are remediated.