

AUDIT REPORT

AUDIT OF THE SMITHSONIAN INSTITUTION NETWORK INFORMATION SYSTEM CONTROLS

Number A-04-05

January 6, 2005



Smithsonian Institution

Office of Inspector General

SUMMARY

The Office of the Inspector General audited Smithsonian Institution (SI) network information system controls. The purpose of the audit was to evaluate SI information system controls for system access, network security, and operating and application system configurations.

The following points were considerations throughout our audit: Adequate security of information and the systems that process it is a fundamental management responsibility. Of necessity, management must strike a reasonable balance between information technology security and operational capability because some controls impede operations. It is Smithsonian policy, as well as good business practice, that controls be established to maintain accountability for the custody and use of resources and to provide reasonable assurance that assets are safeguarded against loss or unauthorized use.

Our review identified network access control security weaknesses within the Smithsonian's publicly accessible network, as well as opportunities to strengthen system configurations for network devices, Windows, and UNIX operating systems and Oracle database applications.

We recommended that the Chief Information Officer establish a process for performing periodic network vulnerability scans of its secure, publicly accessible network; correct server and workstation security holes and close unnecessary network open ports and available services; and ensure network devices, operating systems, and database applications are securely configured to industry standards.

The Chief Information Officer concurred with our recommendations and provided implementation plans. We believe that these implementation plans are responsive to our recommendations.

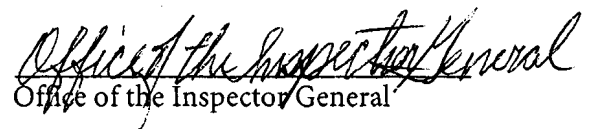

Office of the Inspector General

TABLE OF CONTENTS

	<u>Page</u>
1. Introduction.....	1
A. Purpose.....	1
B. Scope and Methodology	1
2. Results of Audit.....	2
A. Review of Publicly Accessible Network Controls	2
B. Review of Operating Systems and Oracle Database Application Security Configurations.....	7
Appendix A. Policies and Industry Standards.....	12
Appendix B. Management Comments	15

ABBREVIATIONS AND ACRONYMS

NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
SANS	SysAdmin, Audit, Network, Security Institute
SI	Smithsonian Institution
SIRIS	Smithsonian Institution Research Information System

INTRODUCTION

A. Purpose

The purpose of the audit was to evaluate SI information system controls for system access, network security, and operating and application system configurations.

B. Scope and Methodology

The audit was conducted from November 14, 2003, to December 3, 2004, in accordance with generally accepted government auditing standards.

The audit methodology consisted of the following:

- Identifying and reviewing applicable Institution policies and procedures related to general system controls, computer system security, and integrity of computer resources.
- Comparing SI system security settings with industry and Institution standards.
- Evaluating controls meant to safeguard and protect networks.
- Assessing the adequacy of controls meant to prevent and detect unauthorized activities.
- Utilizing guidance issued by the Smithsonian Office of the Chief Information Officer (OCIO), National Institute of Standards and Technology (NIST), National Security Agency, and Microsoft Corporation relating to system security configuration.

Our review also included interviews with SI technology staff, through which we gained an understanding of the practices employed concerning system configuration, network security, and system access.

RESULTS OF AUDIT

A. Review of Publicly Accessible Network Controls

SI network security controls can be strengthened. Specifically, opportunities exist to strengthen controls over network access and configuration settings for network devices. During the audit, OCIO recognized that improvements were needed and has since begun addressing these weaknesses. Until all weaknesses are addressed and corrective plans are in place, SI computers residing on the SI network are at risk of unauthorized access, denial of services, and the unnecessary disclosure of Smithsonian computer system resources information.

Details of Review

As part of our network control testing, we performed external and internal network vulnerability scanning of the SI's secure, publicly accessible network, and other critical SI servers. In addition, we evaluated SI network routers and the primary SI firewall configuration against industry security standards.¹ From our testing, we determined that SI does have network monitoring controls in place. In addition, our testing determined that network access controls could be strengthened to reduce risks such as the unnecessary disclosure of system information. Also, our router and firewall configuration reviews identified that some configuration modifications could strengthen SI network access controls.

Network

As part of our network access control testing, we performed network scans on the internal Smithsonian network and externally from the Internet. In addition, we performed specific network reviews of web servers. From our testing, we identified network weaknesses from the external and internal assessments.

External. We performed external network scans of selected Smithsonian Internet addresses, including the Smithsonian domain name servers.² In addition, we identified the Smithsonian network domain name servers and attempted to determine if a common discovery vulnerability of Smithsonian computer names and addresses, known as a zone transfer, was possible. Our tests were successful in performing a recursive domain name address query. Zone transfers and recursive queries should be prevented because, if successful, the results disclose the names and network addresses of the computers and network devices residing on the network. Knowing the name and network addresses gives an unauthorized user inside information on the network topology naming convention, and therefore possibly the purpose of the computers.

¹ Appendix A contains a summary of policies and industry security standards used during this audit.

² The domain name servers' function is to manage and administer the computer names and addressing for efficient communication across a network. The Smithsonian domain name servers contain approximately 12,000 computers.

From our internal network scans we selected 44 computers that had a range of security holes and vulnerabilities. We also selected specific ports used on the Internet to target from outside the Smithsonian network to determine if the same security holes and vulnerabilities were discoverable. Our testing was successful in identifying 38 of the 44 computers from the Internet and 98 security holes. The majority of these security holes dealt with common web server weaknesses related to ports 80, 443, and 8080. The six remaining computers were successfully filtered by the network firewall.

In addition to an external network scan, we browsed the computers using an internet browser (Microsoft's Internet Explorer, for example) to evaluate the type of information that could be gleaned from them. The browser tests determined that there were numerous systems that leaked system information such as type of server, web application and version, error pages, and browse file directories. The leaking of this type of information is a risk and vulnerability in that unauthorized users of the systems could research and exploit any weaknesses discovered. For example, the Smithsonian Institution Research Information System (SIRIS) Image Server contains various files, directories, and links to another SIRIS system. Following the link, we determined that there were 179 pages of images and files that are downloadable without explicit permissions or adherence to the Smithsonian Copyright statement. In addition, the SIRIS directory structure is identifiable, including a listing of other Smithsonian computer addresses. Also, we discovered a web server used as a test archive server for which we could not ascertain its use or function. The web server's main page states it is used for E-Prints archiving.

Internal. Internally, we concentrated our testing on the Smithsonian secure public network known as the DMZ (demilitarized zone). The secure public network contains those web servers that communicate to the public through the Internet. Our web server testing identified weaknesses in network access, information leakage from a common gateway interface, default page displays, and files containing an account name and password. The following table summarizes our web server reviews.

Web Server Review Summary (19 Servers)	
Finding Type	Total
HTTP ³ Login and Other Remote Access Logins: This includes web pages that permit users to login into the web server.	13
CGI ⁴ Script Access: This includes default common gateway interface test scripts, which should be removed. Unnecessary test scripts increase the vulnerability that the scripts can be executed and possibly allow unauthorized access to the web server.	3
Default/Error Pages: These pages disclose unnecessary information about the web server such as web application, file transfer protocol, and version. This information allows unauthorized users to develop vulnerabilities.	3
Source Code Disclosure: This included discovery of sample directories and web server code that could lead to exploitation or disabling of the web services.	2

³ HyperText Transfer Protocol

⁴ Common Gateway Interface

Also, analyses of our network scans of the secured public network identified 228 hosts with a total of 162 security holes and 809 security warnings.⁵ The majority of these weaknesses stem from ports 80, 443, and 22, as well as from outdated versions of software, failure to apply patches and possible default installations. These ports are used for web services and file transfer purposes.

Routers and Firewall Configuration

As part of our network assessment we evaluated two network devices, the Smithsonian core router (ai-core1) and the primary internet firewall (ai-inet1). While performing the audit, the Office of the Chief Information Officer was in the process of replacing and upgrading its network devices. As a result, the findings presented are generic to a network device and apply to the functions that the router and firewall are performing and, therefore, not directly related to the specific device vendor. From our network device configuration analyses, we determined that several services and configurations could be improved and considered when implementing the latest network devices. For example, we identified seven areas within the configuration of the devices where improvements should be made.

- The first area is remote management through simple network management protocol or SNMP. Enhancements can be made on the access control lists that are in place that would further restrict access to this protocol to only those specific hosts that require it.
- The second area is a common source of trouble that focuses on services that are not necessary for daily operations of the network. Best practices suggest that if a service is not necessary it should be disabled or removed.
- The third area has to do with the Cisco authentication, authorization, and accounting services and the ability to assign specific user rights to an individual. These services help manage the level of privileges each administrator has on the device.
- The fourth area is remote administration via telnet. Whenever possible, remote administration should be performed only through secure encrypted services. The telnet service should be disabled and secure shell should be used in its place as a means of secure authentication and administration.
- The fifth area is the access control lists on the interface lines. This area is perhaps the most critical because this is where the types of traffic allowed into and out of the network are controlled. Specific access control lists need to be put in place that will block known types of Internet-based attacks such as IP spoofing, and distributed denial of service, and that will control which specific hosts have access to resources within the protected network.
- The sixth area is local management of the console and auxiliary ports of the routers themselves. Specific access controls and session timeout values need to be put in place to control who and what type of connection is allowed at these locations.

⁵ A security hole is identified when information can be obtained that would permit an unauthorized user to read a file, determine the directory structure, or gain easy access to the system. A security warning is a misconfiguration, known application, or software weakness that can be exploited.

- The seventh and final area involves remote in-band management through the virtual terminal lines. Specific access controls also need to be put in place that will enforce accountability through individual logins, as well as define which hosts are allowed to connect to device services.

During the audit, OCIO staff recognized that improvements were needed and has since begun addressing these weaknesses. For example, the network infrastructure is in the process of being upgraded into trusted zones, and a more robust firewall and intrusion detection system are being installed. Additional staff has also been added to oversee and monitor network security.

Until all weaknesses are addressed and corrective plans are in place, SI computers residing on the SI network are at risk of unauthorized access, denial of services, and unnecessary information disclosure of Smithsonian computer system resources.

Conclusion

Based upon our network reviews, we believe that the Office of the Chief Information Officer can improve network security by introducing additional vulnerability assessments in its network administration. Implementing periodic security assessments can assist in identifying weaknesses and preventing system compromises.

Recommendations

1. We recommended that the Chief Information Officer establish a process for performing periodic network vulnerability scans of its secure public accessible network.

Management Comments

Concur. OCIO staff is currently analyzing alternative methods and products for performing periodic network vulnerability scanning. OCIO plans to acquire a network scanning product in 2005. The process for performing periodic network vulnerability scanning will be defined in a Technical Note.

Target Completion Date: October 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

2. We recommended that the Chief Information Officer review the identified open ports and available services and close those that are deemed unnecessary.

Management Comments

Concur. OCIO staff will review identified open ports and services and close those that are deemed unnecessary.

Target Completion Date: April 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

3. We recommended that the Chief Information Officer address and correct the server and workstation security holes identified.

Management Comments

Concur. OCIO staff will review the server and workstation security holes identified in the report and correct those that have not already been corrected.

Target Completion Date: April 30, 2005.

4. We recommended that the Chief Information Officer review network device configurations to ensure they are securely configured to industry standards.

Management Comments

Concur. OCIO staff has reviewed network device configuration files to improve security. Beginning in 2005, OCIO will formally review all network device configuration files twice a year or when major changes are made in the network devices. Procedures will be defined and documented in a Technical Note.

Target Completion Date: April 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

B. Review of Operating Systems and Oracle Database Application Security Configurations

SI server operating and application system security configurations can be strengthened. Specifically, both Windows and Solaris UNIX operating systems could be strengthened to industry security standards. This condition exists partially because, at the time of our testing, there were no specific technical configurations for UNIX operating system and Oracle databases. Technical configuration standards have since been developed for UNIX operating systems and Oracle databases. In any event, the systems are vulnerable to unauthorized access and data integrity is at risk.

Details of Review

As part of our system security review we performed security configuration evaluations of operating systems, web service applications, and Oracle databases. From our evaluations we determined that SI systems could be strengthened to meet industry security standards.

Operating Systems

We compared server operating system configurations and settings against Smithsonian and industry standards and guidance. We assessed seven Windows servers and seven UNIX servers' operating systems against these standards. In addition, we used the SANS Top 20 Internet Security Vulnerabilities as a basis for our risk assessment.⁶

For the Windows servers, our evaluation included assessing if security patches and hotfixes were installed and up-to-date for the Windows operating system and, if applicable, for Internet Explorer, Internet Information System, Microsoft Data Component, and Microsoft Media Player. Our evaluations determined that of the 74 operating system configuration tests performed, over 60 percent failed on each server. Specifically, compared to the SANS Top 20 security risks, our analyses revealed that security patches were not up-to-date; password policy was not being followed; registry, directory, and file permissions were not securely set; and that those servers with Internet Information Services installed contained an arbitrary command execution vulnerability.

⁶ The SANS (SysAdmin, Audit, Network, Security Institute) was established in 1989 as a cooperative system security and research and education organization. The SANS Top 20 vulnerability list for Windows and UNIX is composed of the 10 most commonly exploitable vulnerable services for both Windows and UNIX.

The following table summarizes our Windows operating system assessment.

Windows Operating System Reviews								
Servers (a)	1	2	3	4	5	6	7	
RISK LEVELS	1	2	3	4	5	6	7	Average
Total High (b)	8	7	8	8	7	7	7	7
Total Medium (c)	13	13	13	13	13	12	14	13
Total Low (d)	26	26	26	26	26	27	27	26
Total Failed Tests	47	46	47	47	46	46	48	
Total Pass	22	23	22	22	23	23	21	22
Total N/A (e)	5	5	5	5	5	5	5	5
Total Tests	74	74	74	74	74	74	74	
PERCENTAGE FAILURE	64%	62%	64%	64%	62%	62%	65%	
Percentage High Risk Failure	11%	9%	11%	11%	9%	9%	9%	10%
Percentage Medium Risk Failure	18%	18%	18%	18%	18%	16%	19%	18%
Percentage Low Risk Failure	35%	35%	35%	35%	35%	36%	36%	36%
(a) 1: SIERPDW3, 2: SIERPPW1, 3: SIERPPW3, 4: SIERPPW4, 5: SIERPPW2, 6: WEB2, 7: WEB5								
(b) HIGH (Excessive risk): Security risk is high enough to cause a business disruption, if exploited. Also, priority must be given to providing additional resources to reduce risk to an acceptable level.								
(c) MEDIUM (Moderate level of risk): Security risk in conjunction with other events is high enough to cause a business disruption, if exploited. Also, additional resources should be applied to upgrade security to an acceptable level of risk.								
(d) LOW (Low risk): Security risk is high enough to cause operational annoyances or inefficiencies, if exploited. Also, additional resources may be applied to enhance security, but are not required.								
(e) Not-Applicable: Are tests are non applicable for the type of server.								

For the UNIX servers (all were SUN Solaris UNIX versions), we used the UNIX Security Checklist from the Coordination Center at Carnegie Mellon Software Engineering Institute as the industry standard for comparison. From our assessments, we determined that the operating systems were not up-to-date with patches. In fact, all seven had installed patches that, according to the SUN Solaris website, were three months to a year out-of-date. In general, we found that numerous system services were operating at higher than necessary privileges. For example, one of the production enterprise resource planning servers had rlogin, shell, and uucp services⁷ running as default, which is not recommended. Other enterprise resource planning servers had numerous default open ports and services enabled and were running with root permissions such as finger, login, shell, echo, discard, and chargen. The combination of these ports and services makes the system vulnerable to denial of service risks. One of the most severe vulnerabilities involving the enterprise resource planning servers is the ability for remote logon in the highest privileged mode of root. Direct remote logon as root is strictly forbidden by industry standards. Also, the UNIX operating system provides the enabling of password policies; however, these security settings were not enabled or defined by Smithsonian password policy of eight characters, but were set for six characters.

⁷ The rlogin and rsh services establish a remote login session from trusted users without a password challenge. These servers use inadequate authentication based on IP address security (which can be spoofed), domain name service security (which can be spoofed) and the notion of reserved ports (on UNIX systems only user root can open the client port). The uucp is a Unix-to-Unix system copy server, which supports networking over the network. It is used for file copying. It runs as user root and might be compromised. If it is not needed it should be disabled.

The following summarizes the seven UNIX operating systems reviewed.

Solaris UNIX Operating System Reviews								
Servers (*)	1	2	3	4	5	6	7	Average
Total Tests	74	74	74	74	74	74	74	
General Statistics								
Passed	39	39	39	39	38	47	47	41
Failed	26	26	26	26	27	19	19	24
Not Applicable	8	8	8	8	8	7	7	8
% Failed/ Total	35%	35%	35%	35%	36%	26%	26%	33%
%Passed/Total	53%	53%	53%	53%	51%	64%	64%	56%
Detailed Statistics								
Patches Up-to-date (1 Test)0								
Passed								
Failed	x	x	x	x	x	x	x	
Network Services (31 Tests)								
Passed	11	11	11	11	11	17	17	13
Failed	13	13	13	13	13	7	7	11
NA	7	7	7	7	7	7	7	7
Account Security (26 Tests)								
Passed	15	15	15	15	15	18	18	16
Failed	10	10	10	10	10	7	7	9
NA	1	1	1	1	1	1	1	1
File System Security (16 Tests)								
Passed	13	13	13	13	12	12	12	13
Failed	2	2	2	2	3	4	4	3
NA	1	1	1	1	1	0	0	1

(*) 1: SIERP PD1, 2: SIERP PA1, 3: SIERP PA2, 4: SIERP PA3, 5: SIERP PA4, 6: si-webmai01, 7: si-webmail02

Oracle Database

We assessed the Oracle database that supports the enterprise resource planning system against industry security configuration standards. Our assessment included reviewing 51 configuration settings. From our assessments, the Oracle configuration could be strengthened with regard to logging, audit trails, and password encryption and limitations. The following table represents a summary of the configuration tests.

SIERPD1 Oracle Server Summary	
Risk Levels	SIERPD1
Number of High Findings	2
Number of Medium Findings	17
Number of Low Findings	4
Number that Passed Test	27
Not Applicable	1
Number of Test Steps that Failed	23
Total Tests Performed	51
Failure Percentage (Total Failures/Total Tests)	44%
Percentage of High Risk Failure (Total High/Total Tests)	4%
Total Number of Tests	52
Not Tested	1

Conclusion

Based upon our operating system and database configuration reviews, we believe that the Office of the Chief Information Officer can improve its system security configurations by introducing additional vulnerability assessments in its system administration to assist in identifying weaknesses and strengthening system security.

Recommendations

1. We recommended that the Chief Information Officer review the servers and workstations to ensure that all patches and updates are installed for the operating systems and applications.

Management Comments

Concur. OCIO staff will review identified servers and workstations to ensure that uninstalled patches and updates identified in the report have been corrected and take action to install patches and updates where needed.

Target Completion Date: April 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

2. We recommended that the Chief Information Officer review the Windows and UNIX servers to ensure the operating systems are securely configured to industry standards and remove unnecessary services and ports.

Management Comments

Concur. OCIO staff began reviewing Windows and UNIX server configuration files to improve their security in September 2004. Beginning in 2005, OCIO will formally review Windows and UNIX server configuration files twice a year or when major changes are made. Procedures will be defined and documented in a Technical Note.

Target Completion Date: April 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

3. We recommended that the Chief Information Officer review the Oracle database servers to ensure the database application is securely configured to industry standards.

Management Comments

Concur. OCIO staff will review Oracle database servers to ensure that database applications are securely configured.

Target Completion Date: April 30, 2005.

Office of the Inspector General Response

We believe the Chief Information Officer's planned actions, if implemented, are responsive to the recommendation.

Appendix A. Policies and Industry Standards

We evaluated SI system security from November 14, 2003, through December 3, 2004. We used Smithsonian Directives as well as industry guidance and standards from the NIST, Government Accountability Office (formerly the General Accounting Office), National Security Agency, and Microsoft Corporation. The evaluation included a review of server operating system configurations, web server application configurations, databases, user accounts, network ports, and vulnerable services.

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that apply to all Institution units. The directive requires managers to take systematic and proactive steps to develop and implement appropriate, cost-effective management controls. These controls should provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

Smithsonian Directive 931, *Use of Computers & Networks*, August 5, 2002, provides Institution policy on computer safeguards to protect Smithsonian equipment and data. Users are required to use safeguards that include having a password with at least eight alphanumeric and special characters. Passwords must not be found in a dictionary, easily guessed, or left in writing in the user's office. In addition, passwords should be changed every ninety days and not reused.

Smithsonian Institution Office of the Chief Information Officer Technical Note: IT-930-TN02, *Auditing & Logging Procedures*, September 8, 2003, describes the configuration, settings, size and frequency of log review for all auditable systems. This technical note covers all network devices (e.g., routers, switches), network servers, file servers, database servers, application servers, firewalls and intrusion detection systems. The objective is to establish a standard frequency for monitoring audit logs.

Smithsonian Institution Office of the Chief Information Officer Technical Note: IT-930-TN04, *Disabling and Deleting Dormant Accounts*, August 27, 2003, establishes procedures to be used to monitor and disable network accounts at the Smithsonian Institution which have not been used within the last thirty days, and to delete accounts that have been dormant for 180 days.

Smithsonian Institution Office of the Chief Information Officer Technical Note: IT-930-TN08, *Implementing Vendor Software Patches/Fixes*, August 27, 2003, establishes that system administrators or designated technical staff are required to apply security patches or fixes in a timely manner. Patches must be installed on production within seven days of successful completion of testing.

Smithsonian Institution Office of the Chief Information Officer Technical Note: IT-930-TN10, *Minimizing Access to Production Software and Data*, August 27, 2003, establishes procedures by which production data and software can be safeguarded from unauthorized access, modification, and deletion.

Smithsonian Institution Office of the Chief Information Officer Technical Note: IT-930-TN12, *Password Policy Compliance Testing*, August 27, 2003, establishes procedures to be used to verify compliance with established password usage policies (SD 931, *Use of*

Appendix A. Policies and Industry Standards (Continued)

Computers & Networks) at the Smithsonian Institution. The goal is to establish a system of checks and reports that records and monitors the enforcement of password usage.

Smithsonian Institution Office of the Chief Information Officer Technical Note, *Windows 2000 Server Baseline Configuration / Build Notes Application Server Edition Version 1.1*, November 4, 2003, provides setup and configuration guidelines and baselines for the standalone Windows 2000 application servers used in the Smithsonian Institution web infrastructure. The purpose of this guidance is to serve as a step-by-step guide and checklist for building a well-configured and secure Windows 2000 Server with associated infrastructure applications.

Computer Emergency Response Team, Carnegie Mellon Software, *UNIX Security Checklist v2.0*, October 8, 2001, provides detailed steps to improve the security of Unix Operating Systems. It encourages system administrators to review all sections of this document and if appropriate modify their systems accordingly to fix potential weaknesses. If possible, apply this checklist to a system before attaching it to a network. In addition, it is recommended that the checklist be used on a regular basis as well as after installation of any patches or new versions of the operating system.

General Accounting Office (now the Government Accountability Office), *Financial Information Systems Control Audit Manual*, January 1999, provides guidance in evaluating computer-related controls. The guidance describes access controls to provide reasonable assurance that computer resources are protected against unauthorized modifications, disclosure, loss, or impairment. Such controls include physical controls, such as locking computer rooms to limit access. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

National Security Agency, *Guide to Securing Microsoft Windows 2000 File and Disk Resources*, April 19, 2001, recommends that all volumes use new technology file system in order to achieve the highest level of security. Under Windows 2000, only new technology file system supports discretionary access control to the directories and files. New technology file system volumes provide secure and auditable access to the files. Therefore, any file allocation table partitions should be converted to new technology file system.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998, states that the objective of system security planning is to improve the protection of information technology resources. All federal systems have some level of sensitivity and require protection as part of good management practice. According to NIST, system security plans should document the protection of the system.

Appendix A. Policies and Industry Standards (Continued)

Additionally, the completion of system security plans is a requirement of the Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, and Public Law 100-235, *Computer Security Act of 1987*. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place for meeting those requirements. The system security plan also delineates the responsibilities and expected behavior of all individuals who access the system.

NIST, *Guidelines on Securing Public Web Servers*, Special Publication 800-44, September 2002, provides guidelines on securing both Apache and Internet Information Services web server applications. The guidelines include installing permanent fixes (often called patches, hot fixes, service packs, or updates), and removing or disabling unnecessary services and applications. Ideally, a Web server should be on a dedicated, single-purpose host. Many operating systems are configured by default to provide a wider range of services and applications than required by a Web server; therefore, a Web administrator should configure the operating system to remove or disable unneeded services. Some common examples of services that should usually be disabled would include: Windows network basic input/output system (NetBIOS); if not required, file transfer protocol; telnet; simple management transfer protocol; and software development tools.

NIST special publication, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, provides instructions, recommendations, and considerations for government computer security. According to this publication, security policies and procedures should be in place to protect valuable resources, such as information, hardware, and software. The security program should allow for periodic assessments and should ensure that SI system administrators or system security personnel understand their responsibilities.

Appendix B. Management Comments



Smithsonian Institution

Office of the Chief Information Officer

DATE: January 5, 2005

TO: Thomas D. Blair, Inspector General

FROM: *Dennis Shaw*
Dennis Shaw, Chief Information Officer

Cc: S. Burke, B. Daniels

SUBJECT: Response to the Draft Report, Office of the Inspector General Audit A-04-05, Smithsonian Institution Network

Thank you for the opportunity to comment on the draft audit report on the Smithsonian Institution Network. We agree that the Smithsonian Institution Network (SInet) security controls can be strengthened. Since the inception of this audit in November 2003 numerous improvements to network and IT infrastructure security have been implemented. The SInet is considerably more secure than when the audit began.

Planned actions and timelines for completing actions associated with each recommendation are contained in the attachment. If you have any questions, please contact me at 202-633-2800 or Bruce Daniels at 202-633-6000.

Attachment

Appendix B. Management Comments (continued)

Attachment

Smithsonian Institution Network Audit Recommendations

Issue 1: Publicly Accessible Network Controls

Recommendation 1: Establish a process for performing periodic network vulnerability scans of its secure public accessible network.

Comment: Concur. OCIO is currently analyzing alternative methods and products for performing periodic network vulnerability scanning. OCIO plans to acquire a network scanning product in 2005. The process for performing periodic network vulnerability scanning will be defined in a Technical Note.

Target Completion Date: October 30, 2005

Recommendation 2: Review the identified open ports and available services and close those that are deemed unnecessary.

Comment: Concur. OCIO will review identified open ports and services and close those that are deemed unnecessary.

Target Completion Date: April 30, 2005

Recommendation 3: Address and correct the server and workstation security holes identified.

Comment: Concur. OCIO will review the server and workstation security holes identified in the report and correct those that have not already been corrected.

Target Completion Date: April 30, 2005

Recommendation 4: Review network device configurations to ensure they are securely configured to industry standards.

Comment: OCIO has reviewed network device configuration files to improve security. Beginning in 2005, OCIO will formally review all network device configuration files twice a year- or when major changes are made in the network devices. Procedures will be defined and documented in a Technical Note.

Target Completion Date: April 30, 2005

Issue 2: Operating Systems and Oracle Database Application Security Configurations

Recommendation 1: Review the servers and workstations to ensure that all patches and

Appendix B. Management Comments (continued)

updates are installed for the operating systems and applications.

Comment: Concur. OCIO will review identified servers and workstations to ensure that uninstalled patches and updates identified in the report have been corrected and take action to install patches and updates where needed.

Target Completion Date: April 30, 2005

Recommendation 2: Review the Windows and UNIX servers to ensure the operating systems are securely configured to industry standards and remove unnecessary services and ports.

Comment: OCIO began reviewing Windows and UNIX server configuration files to improve their security in September 2004. Beginning in 2005, OCIO will formally review Windows and UNIX server configuration files twice a year- or when major changes are made. Procedures will be defined and documented in a Technical Note.

Target Completion Date: April 30, 2005

Recommendation 3: Review the Oracle database servers to ensure the database application is securely configured to industry standards.

Comment: OCIO will review Oracle database servers to ensure that database applications are securely configured.

Target Completion Date: April 30, 2005