AUDIT REPORT

INFORMATION SYSTEM CONTROLS AT THE NATIONAL MUSEUM OF NATURAL HISTORY

Number A-04-03

September 9, 2004

SUMMARY

The Office of the Inspector General audited information system controls at the National Museum of Natural History (NMNH). The purpose of the audit was to evaluate NMNH information system controls for system access, network security, and operating system configuration. We excluded from this report our assessments of NMNH UNIX and web server applications. These assessments will be reported separately when completed as a follow-on report.

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.

NMNH did have some system security controls in place regarding system backup and network intrusion detection. However, we determined that NMNH network security, operating system configurations, and system access safeguards were inadequate, and that the risk to system access and data integrity was high. During our audit, NMNH management made some system account reviews and changes and began reviewing configuration deficiencies identified during the audit.

We made recommendations to the Director, NMNH and to the Chief Information Officer. We recommended that the Director, NMNH, ensure that staff update NMNH system resources server inventory documentation; address and correct identified network security holes and remove unnecessary open network ports, servers, and user accounts on NMNH servers and workstations; reaffirm the necessity to comply with the Smithsonian Institution password policy; review operating system configurations in Windows servers to ensure that they are securely configured to Office of the Chief Information Officer (OCIO) and industry standards and install missing patches and updates; establish a process to ensure regular oversight of the current NMNH practice permitting NMNH units to establish and administer their own servers, or formalize a reassignment of these responsibilities to a unit that can ensure that these systems are securely configured and administered. We also recommended that the Chief Information Officer clarify the necessity of when and where to place web site links to the Smithsonian privacy policy and copyright restrictions and consider establishing a policy requiring a more secure method of file sharing.

Management agreed with the recommendations and planned actions are responsive to the recommendations.

Office of the Inspector General

Office of the Inspector General

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

ADP	Automated Data Processing
FAT	File Allocation Table
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
NMNH	National Museum of Natural History
NTFS	New Technology File System
OCIO	Office of the Chief Information Officer
SANS	SysAdmin, Audit, Network, Security Institute
SI	Smithsonian Institution
SSH	Secure Shell
SNMP	Simple Network Management Protocol

INTRODUCTION

A. Purpose

The purpose of the audit was to evaluate NMNH information system controls for system access, network security, and operating system configuration.

B. Scope and Methodology

The audit was conducted from November 14, 2003, to August 5, 2004, in accordance with generally accepted government auditing standards. We excluded from this report our assessments of NMNH UNIX and web server applications. These assessments will be reported separately when completed as a follow-on report.

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 NMNH 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, National Institute of Standards and Technology (NIST), National Security Agency, and Microsoft Corporation relating to system security configuration.

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

C. Background

The NMNH opened to the public in March 1910 as the National Museum. NMNH is dedicated to maintaining and preserving the world's most extensive collection of natural history specimens and human artifacts. It also fosters scientific research as well as educational programs and exhibitions that present the work of its scientists and curators to the public.

NMNH Information Technology (IT) administration is composed of two formal units: Automated Data Processing (ADP) and Informatics. We were able to identify approximately 2,800 system resources composed of servers, workstations, printers, and network devices connected to the NMNH network.

RESULTS OF AUDIT

NMNH Information Systems

NMNH systems security can be strengthened to prevent unauthorized access. Specifically, opportunities exist to strengthen controls over network access and server operating systems security configurations and settings.[1] This condition exists because of partial uncoordinated information technology administration across NMNH as well as a lack of oversight and inconsistent compliance with OCIO system administration policies and guidance. Also, according to ADP and Informatics staff, there has been a shortage of staff and insufficient training to effectively manage the complex and diverse information technology needs. As a result, NMNH information systems are vulnerable to unauthorized access and the integrity of its data could be compromised.

Results

We performed internal and external network security reviews of NMNH servers and NMNH client workstations as part of access control testing.[2] In addition, we assessed the server operating systems against industry guidance and configuration standards.[3] From these assessments, we determined that configurations should be modified to meet minimum industry-recommended security configuration standards.

Network Access

Externally and internally, we were successful in identifying some open ports and services that are vulnerable. We were provided with an inventory listing of servers by the NMNH ADP department that identified, for each server listed, the Internet protocol address, resource name, operating system, and unit administration. Comparison of network scans to the server inventory list revealed the listing was incomplete in regards to Internet protocol addresses and operating systems. However, the acting ADP manager stated there have been recent OCIO network address changes that were not reflected in the inventory list. Also, the ADP manager stated he was working on updating the server inventory listing and needed to coordinate with other unit administrators to update the information.

Through our scans and discussions with ADP and the NMNH Informatics webmaster we discovered other servers that were not included in the NMNH server inventory. Moreover, some NMNH server names did not match the documented Internet protocol address. In addition, our network scans discovered other NMNH servers not included in the server inventory or administered by NMNH ADP or Informatics.

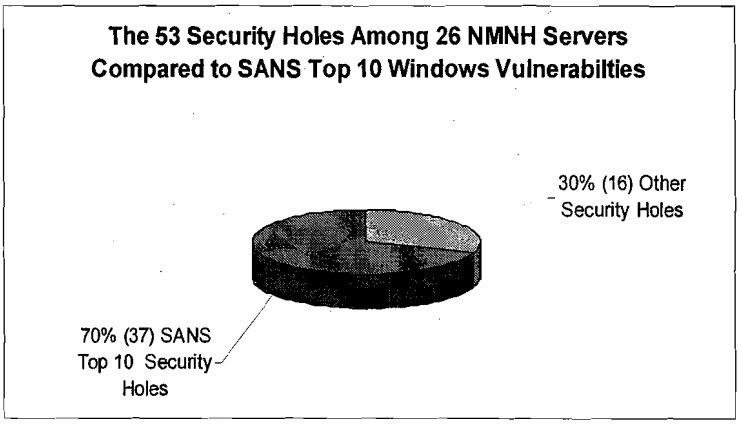
We performed scans of 53 NMNH servers.[4] Analysis of the 53 internally scanned servers revealed 53 security holes, 37 of which, or 70 percent, were related to the SANS Institute

---

[1] See Appendix A, Glossary of technical definitions for an explanation of these and other terms used in this report.
[2] Internal networks are systems accessible within the SI network. External networks are Internet accessible.
[3] Appendix B contains a summary of policies and industry security standards used during this audit.
[4] The 53 NMNH servers consist of 18 Windows, 16 UNIX based, 15 Netware operating system servers, and 4 unconfirmed operating systems. We did not discover vulnerabilities with the Netware servers and concentrated on the Windows servers. Reviews of the NMNH UNIX operating system and Apache web server applications will be addressed in a separate follow-on report.

Top 10 Microsoft Windows vulnerabilities.[5] The major ports and services include NetBIOS and Anonymous logon, Simple Network Management Protocol (SNMP), Secure Shell (SSH), HTTP (Hypertext Transfer Protocol) and FTP (File Transfer Protocol).[6] In performing our review, we did not provide notice of when our network testing was to be performed. However, on numerous occasions NMNH ADP identified our internal network security testing as suspicious activity, which showed some controls are in place to identify suspicious activity within NMNH.

The following chart shows the NMNH server security holes discovered compared to the SANS Top 10 Windows Vulnerabilities. The NetBIOS service, for example, is recognized as a common Windows operating system weakness. Through our testing, we were able to identify 15 of 18 Windows servers which had enabled the NetBIOS protocol. According to NIST 800-43, enabling default Microsoft Windows NetBIOS over certain networks permits the server storage drives to be easily shared and network accessible. Sharing drives across networks is not recommended, unless necessary, because it can permit unauthorized and undetected access to information stored on drives. In addition, according to the SANS, NetBIOS and Simple Network Management Protocol are two of the top 20 most critical Internet security vulnerabilities because they disclose information such as server services, account names, and passwords to unauthorized users.



We were successful in gaining access by exploiting the NetBIOS vulnerability for 13 of the 18 NMNH Windows servers and numerous workstations. Of the 13 Windows servers, we were able to obtain numerous system administrative password accounts. Once we had obtained these accounts, we were able, without authorization, to gain access to the server files and directories. Further analyses of the password files show that some of the administrative passwords were not in compliance with Institution complexity policies, which require the passwords to be at least eight characters and contain a combination of alphanumeric characters and special characters.

We identified vulnerabilities within the NMNH workstations. We performed scans of 13 class "C" networks and identified 711 security holes that were distributed among 39 different services and open ports.[7] Analyses of the workstations compared to the SANS vulnerabilities identified NetBIOS Network Shares, anonymous logon null session, SSH, SNMP, HTTP, FTP vulnerabilities, remote registry access, and remote procedure calls.[8]

---

[5] The SANS (SysAdmin, Audit, Network, Security Institute) was established in 1989 as a cooperative system security research and education organization. The SANS Top 20 vulnerability list for Windows and Unix/Linux includes the 10 most commonly exploited vulnerable services in Windows and the 10 most commonly exploited vulnerable services in UNIX and Linux.

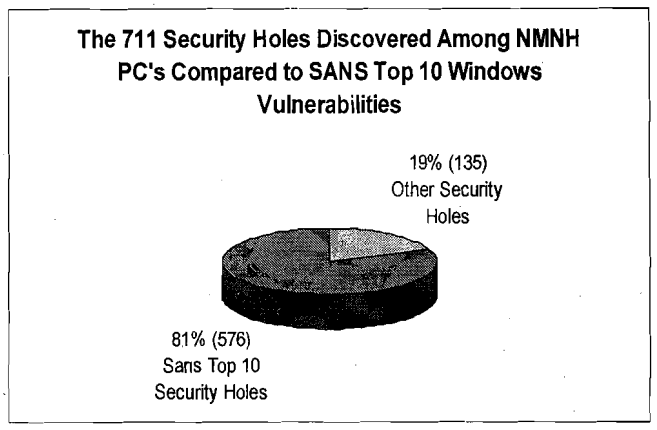
[6] See Appendix A. Glossary

[7] Class "C" networks consisted of 254 addresses each, for a total of 3,302.

[8] See Appendix A. Glossary.

In addition, there was no SI banner warning on most of the computers that had FTP, telnet, and SSH ports and services available.[9]

The following chart shows the comparison of the security holes to the SANS Top 10 Windows vulnerabilities. Workstation access control testing permitted the gathering of password files. Further analyses showed that the passwords were not in compliance with SI policy. Passwords were either blank or the same as the user account. Using administrative accounts, we were able to establish a network path directly to some workstations. We discovered 19 additional web servers upon further analysis of the workstation scans that showed HTTP or port 80 open – a common port used for web servers – that were not included in the NMNH server inventory lists. For example, the following web servers were discovered that were not on the NMNH inventory:



- MSCWEB.si.edu and MSCWEB2.si.edu are intranet web portals for the Museum Support Center.
- WRBU.si.edu is used by Walter Reed Biosystematics Unit as an external web server residing within the SI and NMNH internal network and contained five security holes that include NetBIOS, SSH, HTTP, and two other services.
- VOOM.si.edu is an external web server residing within the SI and NMNH internal network and had two security holes as well as FTP vulnerability. The FTP vulnerabilities permitted our tests to gain access to the server and place files on it externally and internally.
- LMS.si.edu is an internal webserver used by the laboratory of analytical biology and had five security holes, including FTP, SSH, HTTP, and two others.
- SEMANALYSIS.si.edu is an internal webserver that contained two security holes.
- MNMHN-MSPDOC7.si.edu contained one security hole.

We also specifically tested whether NMNH computers (servers and workstations) were vulnerable to the following high-risk Microsoft worm vulnerabilities: remote procedure call, local security authority subsystem service, and SQL (Structured Query Language) Server Resolution.[10] From these tests we identified the following:

- 1 server vulnerable to the remote procedure call worm;
- 364 workstations vulnerable to the RPC (remote procedure call) worm;
- 72 workstations vulnerable to the LSASS (local security authority subsystem service) worm;
- 1 workstation vulnerable to the SQL Server Resolution worm.

[9] See Appendix A. Glossary.
[10] See Appendix A. Glossary.

Web Site Privacy Policy Posting

Through our port scans we identified the common HTTP port 80 used for Internet web servers. We browsed to these computers and identified them as being NMNH websites. Some of these NMNH websites are accessible publicly through the Internet. Our review of these websites found that there was no privacy policy or copyright statement, they contained links to non-SI websites, and these servers were not located within the protected area of the SI network for publicly accessible web servers. Also, discussions with NMNH IT staff revealed that it was unclear whether a link to the SI privacy policy is required on each web page and if there is an SI design standard that should be used by the museums. It is common industry practice as well as an Office of Management and Budget recommendation that federal websites have a clearly posted privacy policy.

Voom.si.edu, for example, is publicly available through the Internet and does not have the SI privacy statement, offers images with no copyright restrictions, and contains links to non-SI websites. We were able to gain administrative access to this website externally through the Internet using FTP and thereby bypass the SI firewall and compromise the SI internal network. Three other websites that are publicly available (ravenel.si.edu, goode.si.edu, and rathbun.si.edu) also do not contain the SI privacy statement.

Server Operating Systems

We compared server operating system configurations and settings against Smithsonian and industry standards and guidance. We sampled 9 of the 18 Windows servers for comparison against SI and industry hardening guidelines (guidelines for securing operating systems and applications). From our analyses we determined the following:

- Security patches and hotfixes were not up to date for operating systems, Internet Explorer, Microsoft Structured Query Language, Microsoft Data Access Components and Remote Procedure Control. However, for some servers that had installed the Internet Information Services application, this application was up to date with patches and hotfixes.
- Directory Access Control is a Windows file and directory auditing feature. These permissions were not optimally set to restrict server file and directory access. Also, we identified one server that was formatted as FAT (file allocation table) and not the recommended NTFS (new technology file system). NTFS offers extensive security permissions and auditing features while FAT does not.
- Protective registry settings were not enabled. Establishing strict permissions for registry settings prevents unauthorized users from altering or modifying the operating system and applications.
- Internet Information Services were not properly configured. Although the servers that contained the Internet Information Services web server application were up to date with patches and hotfixes, additional application security configurations were not set.[11]
- There were numerous user accounts with system administrative privileges whose accounts have not been used within 90 days and whose passwords were older than

[11] The Internet Information Service applications were identified as vulnerable to arbitrary command execution. The command can be used to call arbitrary commands to the web server through a user's web browser. For example, users could use their browsers to execute commands on the web server such as erasing the server's hard drive, thereby bringing down the web server.

the 90-day SI requirement. Upon discovery of this, ADP began to review and remove unnecessary accounts.

The following table summarizes our assessment of the NMNH Windows operating system configurations we reviewed.

NMNH Servers Using Windows Operating System (70 Configuration Settings Tested on Nine Servers)										
Servers	**Avg.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Tests Passed	19	30	21	20	19	18	17	10	19	17
Tests Non-Applicable (a)	2	6	1	0	0	0	0	2	5	0
Tests Failed	49	34	48	50	51	52	53	58	46	53
Total	70	70	70	70	70	70	70	70	70	70
Percentages										
Passed and NA	29%	51%	31%	29%	27%	26%	24%	17%	34%	24%
Failed	71%	49%	69%	71%	73%	74%	76%	83%	66%	76%
Tests Failed by Risk Levels										
High (b)	9	7	8	9	9	10	10	11	7	10
Medium (c)	12	7	11	12	13	13	14	15	10	14
Low (d)	28	20	29	29	29	29	29	32	29	29
Total	49	34	48	50	51	52	53	58	46	53

The nine servers were 1. MNHSYNCSORT, 2. MNHWEBSHIELD, 3. MNHWEBMAIL, 4. ADPWEB, 5. NHBVMASTER, 6. NHADMIN, 7. NHMIS, 8. NHBACK, and 9. NHDATA.
a. Non-applicable tests were not applicable to the type of server being reviewed.
b. High Risk is high enough to cause a business disruption if exploited.
c. Medium Risk in conjunction with another event could cause a business disruption if exploited.
d. Low Risk can cause operational annoyances or inefficiencies if exploited.

NMNH information systems are large, highly diverse, and have numerous SI tenants as well as non-SI tenants with system resources residing on the network. NMNH system administration is spread among different units who have been permitted to establish various systems to support their unit or organizational needs. Although not formalized or overseen, according to ADP staff, these units are responsible for system administration and for complying with SI and OCIO system guidance and requirements. We believe that NMNH system security weaknesses result from partial uncoordinated information technology administration across NMNH as well as from inconsistent compliance with OCIO system administration policies and guidance. Also, according to ADP and Informatics staff, there has been a shortage of staff and insufficient training to effectively manage the complex and diverse information technology needs. NMNH has recognized the need to better coordinate its IT administration and according to the NMNH IT Director, plans are being developed to merge some NMNH IT units into one central unit.

According to industry standards, the weaknesses we identified at NMNH can lead to inadequate access controls that diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. NMNH information systems resources are vulnerable to network and server business disruptions and potential compromises to data integrity.

Conclusion

Based upon our system configuration and network analyses, we believe that NMNH can improve system security by introducing an assessment process into its information technology administration. Implementing security assessments and performing periodic reviews can identify risks, thereby limiting vulnerabilities and preventing system compromises.

Recommendations

We made eleven recommendations to the Director, National Museum of Natural History:

1. We recommended that the Director, National Museum of Natural History, ensure that his staff review the identified open ports and available services and close those that are deemed unnecessary.

Management Comments

Concur. NMNH is currently reviewing all NMNH controlled servers for compliance with OCIO policies and will create a report of the services and ports currently open on each server, to whom, and why. In addition, as part of the migration to at firewall system, NMNH will identify all open ports and services. During the migration period, NMNH will review the open ports and services and determine if any are no longer required and document the business requirement for the ports left open. Target completion date: December 31, 2004.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

2. We recommended that the Director, National Museum of Natural History, ensure that his staff update the server inventory documentation to ensure that all NMNH system resources are accurately accounted for and up-to-date.

Management Comments

Concur. NMNH has begun work to update the server inventory documentation. Target completion date: December 31, 2004.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

3. We recommended that the Director, National Museum of Natural History, ensure that his staff address and correct the server and workstation security holes identified.

Management Comments

Concur. Correcting the high risk server and workstation security weaknesses is a priority for NMNH. Since this work is labor intensive, NMNH will first draft a plan by December 31st that identifies the most cost-effective methodology to mitigate the weaknesses and the resources needed to complete the task Target completion date: May 1, 2005.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

4. We recommended that the Director, National Museum of Natural History, ensure that his staff reaffirm the necessity to comply with the SI password policy across NMNH and non-SI tenants.

Management Comments

Concur. NMNH is committed to achieving compliance with the SI password policy contained in SD 931. NMNH will send an e-mail to all NMNH employees and those from other agencies working in the museum reiterating the SI password policy and commit to reviewing passwords on a quarterly basis consistent with the guidance contained in the SI IT Security Controls Manual. Target completion date: November 30, 2004.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

5. We recommended that the Director, National Museum of Natural History, ensure that his staff review and remove unnecessary accounts on all servers and workstations.

Management Comments

Concur. As a first step, NMNH will review the information provided by the Office of the Inspector General and remove all unnecessary server accounts and revise the passwords to comply with SI password policy for valid server accounts. NMNH will identify unnecessary desktop workstation user accounts and remove them, consistent with the guidance contained in the Smithsonian IT Security Controls Manual. Target completion date: March 31, 2005.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

6. We recommended that the Director, National Museum of Natural History, ensure that his staff review the servers and workstations to ensure that all patches and

updates are installed for the operating systems and applications, beginning with those machines shown to be vulnerable to the high risk Microsoft worm vulnerabilities.

Management Comments

Concur. NMNH is developing a plan for administering Windows servers to include ensuring that upgrades and patches are installed in a timely manner. The high risk vulnerabilities identified in the Inspector General's report will be mitigated by December 31, 2004. Other vulnerabilities will be mitigated as resources allow. Target completion date: December 31, 2004.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

7. We recommended that the Director, National Museum of Natural History, ensure that his staff review publicly accessible NMNH websites for their necessity and consider developing a common design standard.

Management Comments

Concur. NMNH has established a 3-phased project to update the NMNH web pages. The first phase is to implement a common design for the top pages consistent with SI guidance. NMNH is seeking private funding to support the web page redesign. NMNH will also establish a web content steering committee to address web governance and prioritize further investments in web technology. Target completion date: This is expected to be an on-going effort.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation. When the three phases have been implemented and we have been notified, we will consider closing the recommendation.

8. We recommended that the Director, National Museum of Natural History, ensure that his staff relocate publicly accessible web servers off the NMNH and SI intranet to a secure network location.

Management Comments

Concur. Currently the servers that support publicly accessible web sites are supported by either NMNH IT, OCIO, or the departments. The NMNH goal is to create a more secure environment for web hosting, while still giving the departments the flexibility and freedom to create their own content and handle their own development work. To allow for maximum flexibility with the necessary security, NMNH IT will work with OCIO on a plan to relocate the public web sites to OCIO servers using Interwoven's *OpenDeploy* (website content distribution product). The Botany Department will begin a pilot in September that should enable departments to continue to develop web sites locally, but to

push their content to a more secure location for public hosting. Target completion date: June 30, 2005.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

9. We recommended that the Director, National Museum of Natural History, ensure that his staff review operating system configurations in Windows servers to ensure they are securely configured to OCIO and industry standards.

Management Comments

Concur. In conjunction with Recommendation 6, NMNH will review Windows-based server and take steps to securely configure the servers to OCIO and industry standards. Target completion date: March 30, 2005.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

10. We recommended that the Director, National Museum of Natural History, ensure that his staff establish a process to ensure regular oversight of the current NMNH practice permitting NMNH units to establish and administer their own servers, or formalize a reassignment of these responsibilities to a unit that can ensure that these systems are securely configured and administered.

Management Comments

Concur. NMNH will review departmental servers and determine whether the servers should be included in the OCIO application server consolidation project, be administered by the NMNH IT staff, or remain under the control of the individual departments with increased oversight. NMNH will ensure compliance with the IT Security Controls Manual whichever approach is adopted. Target completion date: March 31, 2005.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

11. We recommended that the Director, National Museum of Natural History, ensure that his staff review the IT staffing needs to ensure that staff levels and training needs exist to appropriately administer NMNH system resources.

Management Comments

Concur. NMNH has already begun this review. As a result of this review, NMNH will restructure the organizations that provide IT services. The ADP and Informatics groups are in the process of merging. Other realignments are under consideration. A review of

staffing needs and recommendations on staffing decisions will be provided to the Director and NMNH Executive Staff in September. Target completion date: September 30, 2004.

Office of the Inspector General Response

We believe that the Director's planned actions, if implemented, are responsive to the recommendation.

We made two recommendations to the Chief Information Officer:

1. We recommended that the Chief Information Officer clarify the necessity of when and where to place links to the SI privacy policy and copyright restrictions posted on SI publicly accessible unit websites.

Management Comments

Concur. OCIO has drafted a technical note that establishes the requirement and procedures for including links to the standard Smithsonian Institution copyright notice, privacy notice, and the applicable top Smithsonian web page.

Office of the Inspector General Response

The Chief Information Officer released IT-950-TN01, *Web Copyright and Privacy Notices* prior to the issuance of this report. This action was responsive to the recommendation. Therefore, this recommendation is closed.

2. We recommended that the Chief Information Officer review the use of the file transfer protocol (FTP) and consider establishing a policy requiring a more secure method of file sharing.

Management Comments

Concur. The Smithsonian Computer Security Manager will convene a technical working group to review alternative ways to securely transfer files and implement recommended alternative(s). Target completion date: January 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. Glossary

Anonymous Login Null Session. Anonymous Login Null Session is a network access connection using a blank user name and password.

Application. A complete, self-contained program that performs a specific function directly for the user. This is in contrast to system software such as the operating system which exists to support application programs.

Computer Worm. A computer worm is a piece of computer code that is loaded onto a computer for malicious purposes and often transmits itself from one host to another across a network. Typically, worms and viruses engulf a computer's memory until the system halts.

Directory. A computer system used to organize files on the basis of specific information.

FTP. FTP (File Transfer Protocol) is used extensively as a protocol to transfer files from one computer to another.

Hotfixes. Hotfixes and security patches are intended for enterprise implementations and provide an extra level of security for mission-critical software systems. Specifically, security patches eliminate vulnerabilities by mitigating recognized exploits.

HTTP. HTTP (Hypertext Transfer Protocol) is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

NetBIOS. NetBIOS is part of the Windows networking technology that facilitates the sharing of files and computer resources across a network.

NetBIOS Network Shares. NetBIOS Network Shares are a feature commonly provided on computers running Microsoft Windows that allows the sharing of files or folders across a network with other computers.

Operating System. The software which handles the interface to hardware, schedules tasks, allocates storage, and presents a default interface to the user when no application program is running.

Remote Registry Access (RAC). Remote Registry Access is the ability to remotely access the registry settings that are used to manage software, device configurations, and user settings.

Remote Procedure Calls (RPC). Remote Procedure Call is the ability for one computer to access another computer and execute arbitrary code on that computer.

Security Hole. A security hole is a security weakness that permits a computer intruder to get access to files or walk through the file system. A security warning is a weakness that can be exploited in conjunction with a vulnerability.

Server. A computer or device which provides some service for other computers connected to it via a network. For example, a file server is a computer and storage device dedicated to storing files and sharing those files over a network. A print server is a computer or device that manages one or more printers, while a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

Simple Network Management Protocol. Simple Network Management Protocol (SNMP) is used extensively to remotely manage and configure devices such as printers, network routers, and to monitor network services.

SSH. SSH or Secure Shell is a popular service for securing system logins, command execution, and file transfers across networks.

System Administrator. An individual responsible for maintaining a computer system, including a local-area network. Typical duties include: adding and configuring new workstations, setting up user accounts, installing system-wide software, and performing procedures to prevent the spread of viruses.

Protocol. When data is being transmitted between two or more devices, something needs to govern the controls that keep this data intact. A protocol is a formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces or high-level exchanges between application programs.

Warning banner. A warning banner is a screen with text that gives notice to individuals who are accessing a computer.

Web server. A web server is an application running on a computer which sends out web pages in response to requests from remote network or Internet users.

Appendix B. Policies and Industry Standards

We evaluated NMNH system security from November 14, 2003, through August 5, 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

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 including: 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 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 a setup and configuration guideline and baseline for the standalone Windows 2000 application servers used in Smithsonian Institution web infrastructure. The purpose of this guideline is to serve as a step-by-step guide and check-list for building a well configured and secure Windows 2000 Server with associated infrastructure applications.

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, *Research, Study by Trusted Systems Services, Windows NT Security Guidelines Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments,* 1999, provides guidelines for countering known attacks on Windows NT installations that maliciously expose or modify user data. The goal is to make Windows NT as secure as reasonably and practically possible. Implicit in the guidelines is the understanding that recommendations must be both effective against certain threats and also practical. A balance is necessary between security and operations because some controls impede operational capability.

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.

National Security Agency, *Guide to Securing Microsoft Windows NT Networks,* 2001, identifies a variety of available Windows NT 4.0 security mechanisms and describes measures for their implementation. The guide provides step-by-step instructions on how to utilize the operating system's built-in security features.

Appendix B. Policies and Industry Standards (Continued)

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.

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 personnel understand their respective responsibilities.

Microsoft White Paper, *Securing Windows NT Installation*, 1997, states that the default, out-of-the-box NT configuration is unsecured, and discusses various security issues with respect to configuring all Windows NT operating system products.

Appendix C. Management Comments

Smithsonian
National Museum of Natural History

Date August 25, 2004

To Tom D. Blair, Inspector General

cc Sheila Burke, Deputy Secretary and Chief Operating Officer
David Evans, Under Secretary for Science

From Cristián Samper, Director, National Museum of Natural History
Dennis R. Shaw, Chief Information Officer

Subject Response to the Draft Report, Office of the Inspector General Audit A-04-03, Information System Controls at the National Museum of Natural History

Thank you for the opportunity to comment on the draft audit report on the Information System Controls at the National Museum of Natural History. We agree with the audit findings and the report recommendations. Planned actions and timelines for completing actions associated with each recommendation are contained in the attachment.

Please direct any questions you may have regarding this response to Bruce Daniels, OCIO Computer Security Manager, at 202-633-6000 or Carol Fiertz, NMNH IT Manager, at 202-633-0768

Recommendations to the Director, National Museum of Natural History:

Recommendation 1: Review the identified open ports and available services and close those that are deemed unnecessary.

Comment: Concur. NMNH is currently reviewing all NMNH controlled servers for compliance with OCIO policies and will create a report of the services and ports currently open on each server, to whom, and why. In addition, as part of the migration to the Checkpoint firewall system, NMNH will identify all open ports and services. During the migration period, NMNH will review the open ports and services and determine if any are no longer required and document the business requirement for the ports left open.

Target Completion Date: December 31, 2004

Recommendation 2: Update the server inventory documentation to ensure all NMNH system resources are accurately accounted for and up-to-date

Comment: Concur. NMNH has begun work to update the server inventory documentation.

Target Completion Date: December 31, 2004

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

Comment: Concur. Correcting the high risk server and workstation security weaknesses is a priority for NMNH. Since this work is labor intensive, NMNH will first draft a plan by December 31st that identifies the most cost-effective methodology to mitigate the weaknesses and the resources needed to complete the task.

Target Completion Date: May 1, 2005

Recommendation 4: Reaffirm the necessity to comply with the SI password policy across NMNH and non-SI tenants.

Comment: Concur. NMNH is committed to achieving compliance with the SI password policy contained in SD 931. NMNH will send an email to all NMNH employees and those from other agencies working in the museum reiterating the SI password policy and commit to reviewing passwords on a quarterly basis consistent with the guidance contained in the SI IT Security Controls Manual.

Target Completion Date: November 30, 2004

Recommendation 5: Review and remove unnecessary accounts on all servers and workstations.

Comment: Concur. As a first step, NMNH will review the information provided by the

OIG and remove all unnecessary server accounts and revise the passwords to comply with SI password policy for valid server accounts. NMNH will identify unnecessary desktop workstation user accounts and remove them, consistent with the guidance contained in the Smithsonian IT Security Controls Manual.

Target Completion Date: March 31, 2005

Recommendation 6: Review the servers and workstations to ensure all patches and updates are installed for the operating systems and applications beginning with those machines shown to be vulnerable to the high risk Microsoft worm vulnerabilities.

Comment: Concur. NMNH is developing a plan for administering Windows servers to include ensuring that upgrades and patches are installed in a timely manner. The high risk vulnerabilities identified in the IG report will be mitigated by December 31, 2004. Other vulnerabilities will be mitigated as resources allow.

Target Completion Date: December 31, 2004

Recommendation 7: Review those publicly accessible NMNH websites for their necessity and consider developing a common design standard.

Comment: Concur. NMNH has established a 3-phased project to update the NMNH web pages. The first phase is to implement a common design for the top pages consistent with SI guidance. NMNH is seeking private funding to support the web page redesign. NMNH will also establish a web content steering committee to address web governance and prioritize further investments in web technology.

Target Completion Date: This is expected to be an on-going effort.

Recommendation 8: Relocate publicly accessible web servers off the NMNH and SI intranet to a secure network location.

Comment: Concur. Currently the servers that support publicly accessible web sites are supported by either NMNH-IT, OCIO, or the departments. The NMNH goal is to create a more secure environment for web hosting, while still giving the departments the flexibility and freedom to create their own content and handle their own development work. To allow for maximum flexibility with the necessary security, NMNH-IT will work with OCIO on a plan to relocate the public web sites to OCIO servers using *Interwoven*'s *OpenDeploy*. The Botany Department will begin a pilot in September that should enable departments to continue to develop web sites locally, but to push their content to a more secure location for public hosting.

Target Completion Date: June 30, 2005

Recommendation 9: Review operating system configurations in Windows servers' to ensure they are securely configured to OCIO and industry standards.

Comment: Concur. In conjunction with Recommendation #6, NMNH will review

Windows-based server and take steps to securely configure the servers to OCIO and industry standards.

Target Completion Date: March 30, 2005

Recommendation 10: Establish a process to ensure regular oversight of the current NMNH practice permitting NMNH units to establish and administer their own servers or formalize a reassignment of these responsibilities to a unit that can ensure these systems are securely configured and administered.

Comment: Concur. NMNH will review departmental servers and determine whether the servers should be included in the OCIO application server consolidation project, be administered by the NMNH IT staff, or remain under the control of the individual departments with increased oversight. NMNH will ensure compliance with the IT Security Controls Manual whichever approach is adopted.

Target Completion Date: March 31, 2005

Recommendation 11: Review the IT staffing needs to ensure staff levels and training needs exist to appropriately administer NMNH system resources.

Comment: Concur. NMNH has already begun this review. As a result of this review, NMNH will restructure the organizations that provide IT services. The ADP and Informatics groups are in the process of merging. Other realignments are under consideration. A review of staffing needs and recommendations on staffing decisions will be provided to the Director and NMNH Executive Staff in September.

Target Completion Date: September 30, 2004

Recommendations to the Chief Information Officer:

Recommendation 1: Clarify the necessity of when and where to place links to the SI privacy policy and copyright restrictions posted on SI publicly accessible unit websites.

Comment: Concur. OCIO has drafted a technical note that establishes the requirement and procedures for including links to the standard Smithsonian Institution copyright notice, privacy notice, and the applicable top Smithsonian web page. The Office of General Council and the Office of Public Affairs are reviewing the proposed guidance.

Completion Date: September 30, 2004

Recommendation 2: Review the use of the file transfer protocol (FTP) and consider establishing a policy requiring a more secure method of file sharing.

Comment: Concur. The Smithsonian Computer Security Manager will convene a technical working group to review alternative ways to securely transfer files and implement recommended alternative(s).

Completion Date: January 30, 2005