AUDIT REPORT

INFORMATION SYSTEM CONTROLS AT THE NATIONAL MUSEUM OF AMERICAN HISTORY, BEHRING CENTER

Number A-04-02

June 16, 2004

SUMMARY

The Office of the Inspector General audited information system controls at the National Museum of American History, Behring Center (NMAH). The purpose of the audit was to evaluate NMAH information system controls for system access, server and database configurations, and network security.

Two points were considered throughout our audit: (1) Adequate security of information and the systems that process it is a fundamental management responsibility. (2) Management must, of necessity strike a reasonable balance between information technology security and operational capability because some controls impede operations.

Smithsonian policy, requires managers to establish adequate controls to maintain accountability for the custody and use of resources and to provide reasonable assurance that assets are safeguarded against loss or unauthorized use. Overall, NMAH did have system backup security controls in place. However, we determined that NMAH system security configurations and safeguards were inadequate and that the risk to system access and data integrity was high. During our audit, NMAH management reviewed system accounts, made changes, and began reviewing configuration deficiencies identified during the audit.

We made recommendations to improve systems security and general system controls at NMAH. The recommendations included performing reviews of system configurations; removing unnecessary accounts; developing plans to address identified system security weaknesses; and establishing policies and minimum technical configuration guidance for server operating systems, web server applications, and databases. Management agreed with the recommendations and planned actions are responsive to the recommendations.

Office of the Inspector General

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

NIST	National Institute of Standards and Technology
NMAH	National Museum of American History, Behring Center
SANS	System, Audit, Network, Security Institute

INTRODUCTION

A. Purpose

The purpose of the audit was to evaluate NMAH information system controls for system access, server and database configurations, and network security.

B. Scope and Methodology

The audit was conducted from November 14, 2003, to May 7, 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 system general controls, computer system security, and integrity of computer resources.
- Comparing NMAH 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 National Institute of Standards and Technology (NIST), National Security Agency, Oracle Corporation, and Microsoft Corporation relating to system security configuration.

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

C. Background

The NMAH opened to the public in January 1964 as the Museum of History and Technology. NMAH's basic mission is the collection, care, and study of objects that reflect the experience of the American people.

RESULTS OF AUDIT

Review of NMAH Information System Security

NMAH systems security can be strengthened to prevent unauthorized access. Specifically, opportunities exist to strengthen controls over network access, server operating systems, databases, and web server applications security configurations and settings. This condition exists because of a lack of specific system configuration standards and inadequate NMAH information technology staff resources to address system security weaknesses. As a result, NMAH information systems are vulnerable to unauthorized access and the integrity of its data could be compromised.

Network Access

We scanned external and internal network ports and services of NMAH servers as part of access control testing. Internally, we also scanned and performed limited penetration testing of NMAH client workstations. In addition, we assessed the server operating systems, databases, and web server applications against industry guidance and configuration standards.[1] From these assessments, we determined that configurations should be modified to meet minimum industry recommended security configuration standards. Also, we performed scans of 13 NMAH servers.[2] Externally, we were unsuccessful in identifying the specific ports and services at the time we conducted our tests for these servers. Our internal network scans, however, did find some open ports with available services that could be vulnerable. Our scans of client workstations discovered vulnerabilities. One in particular allowed access to sensitive data such as personnel, marketing, and sponsor fundraising information.

Analysis of the 13 internally scanned servers revealed 21 security holes and 47 security warnings.[3] The major ports and services include NetBIOS, Simple Network Management Protocol, OpenSSL, and File Transfer Protocol. The NetBIOS service, for example, is recognized as a common Windows operating system weakness. We were able to identify eight of nine Windows servers which had enabled the NetBIOS protocol.[4] According to industry standards, enabling default Microsoft Windows NetBIOS over certain networks permits the server storage drives to be easily shared and accessible. Sharing drives across networks is not recommended, unless necessary, because it can permit unauthorized and undetected access to information. In addition, according to the System, Audit, Network, Security Institute (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.

Through our access control testing we were successful in exploiting the NetBIOS vulnerability for seven of the eight NMAH Windows servers and numerous work stations. Of the seven Windows servers, we were able to obtain 29 system administrative password

---

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

[2] The 13 NMAH servers consist of 9 Windows and 4 Netware operating system servers. We were unable to discover vulnerabilities with the Netware servers and concentrated on the Windows servers.

[3] A security hole is a security weakness that permits a computer intruder to get instant access to read any file or walk through the file system. A security warning is a weakness that can be exploited in conjunction with a vulnerability.

[4] NetBIOS is part of the Windows networking technology and represents a large share of common network level exploits that includes the sharing of files across a network.

accounts. Once we had obtained these accounts, we were able, without authorization, to gain access to the server and the files and directories that contained the Collection Management Database and an NMAH financial system database. A review of the password files determined that some of the 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 a special character[5]. For example, one particular system backup account provided access to most of NMAH servers by itself. Also, the default administrative account was often not renamed as required by Institution policy and industry guidance.

Server Operating Systems

We compared server operating system and database configurations and settings against industry standards and guidance. We concentrated on six of the nine Windows servers. We encountered technical difficulties in executing scripts against the remaining three Windows servers.[6] NMAH had not enabled some of the Windows servers as new technology file systems (NTFS) for three of its servers (AHBFMS, MIMSYWEB, and NMAH-312688). Instead, the servers were using the file allocation table (FAT).

The new technology file system offers extensive security permissions and auditing features that can be customized at the file and directory levels, as opposed to the file allocation table, which does not permit full utilization of these advanced security features. As a result, we were unable to fully assess the operating system configurations. Windows new technology file system is the file system recommended by the National Institute Standards and Technology (NIST) for Windows operating systems because of the additional security settings it offers. In addition, our assessments revealed that operating system patches and hot fixes were not up to date.

[5] Special characters are key board characters such as !@#$%^&*().

[6] A script is a file that is executed on a computer that will automatically gather certain settings and configurations. These data are further analyzed for comparison to industry system security standards.

The following table summarizes our assessment of the NMAH Windows operating systems.

NMAH Servers Using Windows Operating System (70 Configuration Settings Tested)						
Servers	**AHBFMS**	**AHBWEB**	**MIMSYWEB**	**NMAH-312668**	**FMSWEB**	**AHBMIMSY**
Tests Passed	12	13	13	13	21	13
Tests Non-Applicable (a)	9	3	8	8	1	2
Tests Failed	49	54	49	49	48	55
Total	**70**	**70**	**70**	**70**	**70**	**70**
Percentages						
Passed and NA	30%	23%	30%	30%	31%	21%
Failed	70%	77%	70%	70%	69%	79%
Tests Failed by Risk Levels						
High (b)	8	8	8	8	7	8
Medium (c)	11	15	12	12	13	15
Low (d)	30	31	29	29	28	32
Total	**49**	**54**	**49**	**49**	**48**	**55**

a. Non-Applicable are tests that were not applicable to the type of server being reviewed.
b. High (Excessive Risk) Risk is high enough to cause a business disruption if exploited.
c. Medium (Moderate Risk) Risk in conjunction with another event could cause a business disruption if exploited.
d. Low (Low Risk) Risk can cause operational annoyances or inefficiencies if exploited.

Database Applications

We determined that two NMAH Oracle databases contained numerous administrative default installation accounts, passwords, user profiles, and assignments.[7] These administrative accounts provide the access and ability to modify and delete database information. According to industry standards and Institution policy, default accounts or passwords should be removed, renamed, or changed. Also, some accounts were unknown to NMAH technology staff, and other accounts represented users who have left the Institution but whose accounts and system access were still enabled.

Web Server Applications

We compared web server application configurations with industry standards. NMAH uses both Internet Information Systems and Apache for their web server applications.[8] We determined that three NMAH web servers had significant weaknesses: they were not configured and updated to the most current versions; they contained questionable installed protocols such as NetBIOS; they contained default installation files and directories; and they contained default accounts with anonymous access privileges. NIST

[7] These databases are used to support the NMAH collection system (MIMSY) and the NMAH financial management system (FMSWEB).
[8] Web server applications are used for computers that are used for internet purposes.

recommends that default installation files, directories, accounts, and anonymous access privileges be removed. Finally, the current configuration of these three web servers allows unauthorized users the ability to obtain file and directory locations.

We believe NMAH system security weaknesses result from the lack of Institution-specific technical baseline configuration standards and guidance, as well as from the lack of resources (staff and budgetary) necessary to support the NMAH's technology needs. The Institution has not issued policies or minimum technical configuration guidance for servers and databases for most versions of Windows operating systems, web server applications, and databases. In addition, within the last two years NMAH information technology administrative staff was reduced and reassigned to the Office of the Chief Information Officer. The staff position was not replaced, and according to NMAH information technology staff, the responsibilities for this position are still needed to maintain NMAH systems up to date and configured correctly. Also, some of the system weaknesses were known and have not been addressed due to budgetary constraints. For example, a security remediation plan for the NMAH Collection Management System server is specifically part of the annual security budget request to the Office of Management and Budget. The remediation plan outlines the system weaknesses and recommended solutions.

According to industry security standards, inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. With the weaknesses our audit identified, NMAH information system resources are vulnerable to network and server business disruptions; potential data integrity compromises for its major databases; compromises of personnel, marketing, fundraising and donor information; and loss of web services.

Conclusion

Based upon our system configuration and network analyses, we believe that NMAH 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 recommended that the Director, National Museum of American History, Behring Center ensure that his staff:

1. Perform periodic reviews of server security configurations to ensure patches and hot fixes are up to date for operating systems, web server applications, and databases.

2. Establish a process to ensure that unnecessary accounts are removed expeditiously from system resources.

3. Perform regular network scans of NMAH networks to identify and close unnecessary ports and services.

4. Reiterate the need for all NMAH users to comply with the Institution's computer password policy.

5. Develop a plan to begin addressing identified security weaknesses for its major systems.

Management Comments

NMAH management concurred with all of our recommendations. NMAH staff plans to upgrade its operating systems to the Office of the Chief Information Officer baseline during FY 2004. By June 30, 2004, NMAH plans on completing and removing unnecessary system accounts. NMAH plans to acquire tools and train staff to perform periodic network scans. NMAH plans to issue a semiannual email notification to all NMAH staff regarding strong password compliance. NMAH staff will develop a plan of action and milestone report for the Collection Information System.

Office of the Inspector General Response

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

Recommendation

We recommended that the Chief Information Officer establish policies and minimum technical configuration guidance for server operating systems, web server applications, and databases.

Management Comments

The Chief Information Officer concurred with our recommendation. The Chief Information Officer stated that he has developed and issued configuration standards and guidance for Windows 2000 servers. At the time of the audit, no other Windows operating system complied with the Smithsonian's Technical Reference Model. The Institution does not currently have specific configuration guidelines for web servers using Apache or for database servers but plans on completing configuration guidelines by the end of fiscal year 2004.

Office of the Inspector General Response

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

Appendix A. Policies and Industry Standards

We evaluated NMAH systems security during November 14, 2003, through May 7, 2004. We used Smithsonian Directives as well as industry guidance and standards from the NIST, 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 alphabetic numeric, and special characters. Passwords must not be found in a dictionary, easily guessed, or left in writing in the user's office. Also, passwords should be changed every 90 days and not reused.

National Security Agency, *Guide to the Secure Configuration and Administration of Oracle9i Database Server,* September 30, 2003, Version 1.2, describes how to securely configure and administer the Oracle9i Enterprise Edition Database Server. This guide must be supplemented with The Center for Internet Security's Oracle Database Security Benchmark v1.0.

The Center for Internet Security, *Oracle Database Security Benchmark v1.1* provides high-level recommendations to secure an Oracle database with a baseline configuration to protect the system from the common "out of the box" vulnerabilities. The security of the Oracle database is a function of the security of the network and operating system that hosts the database. The guidance recommends that all relevant security patches be installed.

General Accounting 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 expose or modify user data maliciously. 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 the new technology file system be used 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 a solid security foundation for any Windows NT 4.0 network by offering step-by-step instructions on how to utilize the operating system's built-in security features.

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.

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 B. Glossary

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.

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

Hot Fixes. Hot fixes 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.

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

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.

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 vulnerability.

Server. A computer 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 that manages one or more printers, and 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 the protocol governing network management and the monitoring of network devices and their functions.

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 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.

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

Appendix C. Management Comments

Smithsonian
National Museum of American History
Behring Center
Office of the Director

Memo

Date May 21, 2004

To Thomas D. Blair, Inspector General

From Brent Glass, Director National Museum of American History

Cc Sheila Burke, COO
Dennis Shaw, CIO
William Hoyt, IG
Dennis Dickinson, NMAH

Subject NMAH Information Systems Controls Audit

This IT systems controls audit expands our knowledge of the extent to which our systems and electronic data are at risk. We learned a great deal from the FY2003 risk assessment of our Collections Information System (CIS). The FY2004 remediation tasks established by that assessment are to begin shortly and will address some of the issues raised in your report. Plans to rebuild servers in our datacenter after OCIO consolidation will resolve others.

As mentioned in your summary, NMAH IT staff began addressing some of the vulnerabilities as soon as they were discovered. But it will take time to examine the contents of all reports that were delivered; we need to identify which weaknesses are urgent, which are "false-positive", and whether the remedy of any will negatively impact the operation of critical systems or applications.

At this time, we affirm the facts presented in the report and respond to each recommendation as follows:

- **Perform periodic reviews of server security configurations to ensure patches and hot fixes are up-to-date for operating systems, web server applications, and databases.**
  - Server security operating system and antivirus configurations are periodically assessed. The April 2004 Sasser worm attack was thwarted by operating system updates applied to all our Windows servers in March 2004.
  - Our preference is to implement software tools to automatically maintain system and security configurations. Many of the recently replaced desktop PCs receive system patches from the OCIO SUS server. Our plan is for all NMAH systems to

be configured this way in the future.
- NMAH plans to upgrade the operating systems of several servers identified in the report to OCIO baselines during FY2004.

- **Establish a process to ensure unnecessary accounts are removed expeditiously from system resources**
  - Work has begun to remove or disable unnecessary server operating system and database accounts.
  - The existing process will be reviewed and updated to conform to SI guidelines by June 30, 2004.

- **Perform regular scans of NMAH networks to identify and close unnecessary ports and services**
  - NMAH will need to acquire tools and train/hire technical staff to conduct this task on a quarterly basis.
  - Guidance is needed from the OCIO security office on what ports and services are deemed unnecessary. This must be cross-checked against the NMAH portfolio of applications to determine if there are known conflicts.

- **Reiterate the need for all NMAH users to comply with the Institution computer password policy**
  - NMAH will issue bi-annual "strong password" e-mail compliance notifications to staff.
  - Every NMAH user is required to comply with the Institution's password and computer/network usage policies. The password policy is specifically referenced in Part 8 of the SI/NMAH Network/Application User Account application that must be signed to obtain a network/e-mail/database account.
  - Annual "Computer Security Awareness" training compliance is monitored
  - 90 day password aging is implemented

- **Develop a plan to begin addressing identified security weaknesses for its major systems.**
  - NMAH will develop a POA&M by August 30, 2004 to begin addressing weaknesses not identified in the CIS POA&M.

Appendix C. Management Comments (continued)

Smithsonian Institution — Memo

Office of the Chief Information Officer

Date: May 25, 2004

To: Thomas D. Blair
Inspector General

cc: Sheila Burke

From: Dennis Shaw
Chief Information Officer

Subject: Response to the IG's Draft Report on NMAH Information System Controls

Thank you for the opportunity to comment on the draft audit report on the NMAH Information Systems Controls Review. We agree with the report recommendations. However, we disagree with the underlying causes of the weakness identified in the draft IG report. We believe that the weaknesses have more to do with compliance with existing policies, procedures, and standards. Specific comments are attached.

Please call me on 202-633-2800 or Bruce Daniels on 202-633-6000 if you have any questions.

Attachment

Arts & Industries Building Room 2361
900 Jefferson Drive SW
Washington, DC 20560-0463
202.633.2800 Telephone
202.312.2884 Fax

Attachment

Response to Draft Audit Report on NMAH Information System Controls

Draft Report: "We believe NMAH system security weaknesses are due to the lack of Institution specific technical baseline configuration standards and guidance, as well as to the lack of resources (staff and budgetary) necessary to support the Museum technology needs. The Institution has not issued policies or minimum technical configuration guidance for servers and databases for most versions of Windows operating systems, web server applications,and databases."

OCIO Comment: The OCIO has developed and issued configuration standards and guidance for Windows 2000 servers. At the time of this audit, no other Windows operating system complied with the Smithsonian's Technical Reference Model (TRM). The configuration guidelines specified configuration standards for Windows 2000 servers and for web servers deployed using Microsoft IIS. SI does not currently have specific configuration guidelines for web servers using Apache or for database servers. Numerous other guidelines are in place that had they been followed, would have prevented many of the weaknesses addressed in the Audit. The IT Security Controls manual identifies a number of controls to be implemented. Among these are Auditing and Logging Procedures (IT-930-TN02); Disabling and Deleting dormant Accounts (IT-930-TN04); Implementing vendor Software Patches/Fixes (IT-930-TN08); Minimizing Access to Production Software and Data (IT-930-TN10); and Password Policy Compliance Testing(IT-930-TN12).

Draft Report: "In addition, within the last two years NMAH information technology administrative staff was reduced and reassigned to the Office of the Chief Information Officer. The staff position was not replaced, and according to NMAH information technology staff, the responsibilities for this position are still needed to maintain NMAH systems up to date and configured correctly."

OCIO Comment: The draft report leaves the impression that theone individual, FTE, and funds for the position were reassigned from NMAH to OCIO. This is not the case. The NMAH employee filled a vacancy within the OCIO Network Management Division. NMAH management chose to redirect the FTE and funds to resolve other priority needs

Draft Report: "Also, some of the system weaknesses were known and have not been addressed due to budgetary constraints. For example, a security remediation plan for the NMAH Collection Management System server is specifically part of the annual security budget request to the Office of Management and Budget. The remediation plan outlines the system weaknesses and recommended solutions."

OCIO Comment: NMAH did not ask for an increase in the FY 2006 budget request to address IT security for its Collection Information System or IT operations. Progress toward eliminating security weaknesses is reported to OMB through the quarterly and annual reporting required by the Federal Information Security Management Act (FISMA) and is not partof the OMB budget submission. Many of the weaknesses identified in the audit report were previously identifiedin the NMAH CIS security remediation plan (POA&M) and should have already been corrected. Many of the most significant security fixes can easily be undertaken and will not require significant budgetary allotments.

Smithsonian
Office of the Chief Information Officer

Memo

Computer Security Staff

Date June 7, 2004

To David Cole, IT Audit Supervisor

From Bruce Daniels, Director Computer Security Staff

Through Dennis Shaw, Chief Information Officer

Subject IT configuration documents

OCIO acknowledges the significance of configuration guidelines. We are currently in the process of completing a series of configuration guidelines for a variety of servers and operating systems. We have currently completed configuration guidelines for Windows 2003 server, as well Windows 2000 servers and IIS. We expect to complete configuration guidelines for UNIX; SQL server; Oracle server; and Apache server by the end of fiscal year 2004.

SMITHSONIAN INSTITUTION
Natural History Building Room EG-15
10th Street and Constitution Avenue NW
Washington DC 20560-0136
202 357 1555 Telephone
202 357 4155 Fax