

AUDIT REPORT

NATIONAL MUSEUM OF THE AMERICAN INDIAN INFORMATION SYSTEMS

Number A-02-06

January 17, 2003



Smithsonian Institution

Office of Inspector General

SUMMARY

The Office of the Inspector General audited information system security at the National Museum of the American Indian (NMAI). With the opening of the new Mall Museum approaching, NMAI requested a comprehensive review of its information security program. The purpose of the audit was to evaluate information system controls regarding server and network security, application developments, service continuity, segregation of duties, and physical conditions.

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.

Overall, NMAI did have some system security controls in place regarding system backup, systems audit trails and server password security features operating. However, we determined that NMAI system security configurations and safeguards were inadequate and the risk to system access and data integrity was high. During our audit, NMAI management made some system account reviews and changes and began reviewing configuration deficiencies identified during the audit. 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. Therefore, we made 24 recommendations to improve systems security and general system controls at NMAI and 2 recommendations to the Smithsonian Institution Chief Information Officer. The recommendations to NMAI include:

- developing and implementing technical industry guidance for server and client configuration settings;
- defining technology positions to include system security responsibilities;
- reviewing the current system configurations and making adjustments deemed necessary to enhance system security;
- defining an NMAI sponsor and formally defining a development implementation team for the collection management system, media information management, and contact management system; and
- assigning contract oversight responsibilities for evaluating technical changes to qualified information technology staff.

The two recommendations to the Chief Information Officer include:

- issuing policies and guidance on the use of peer-to-peer technology for the Institution; and
- modifying the Smithsonian Institution network control points to identify large files transfers and potential file sharing activities in order to alert network administrators.

Both the Director of the National Museum of the American Indian and the Chief Information Officer generally agreed with the audit recommendations. We recommend that the Director provide clarification for three recommendations. Overall, we believe that the corrective actions taken are responsive to the recommendations. For those recommendations requiring additional implementation plans, we plan to follow up with the Director.

Office of the Inspector General
Office of the Inspector General

TABLE OF CONTENTS

	<u>Page</u>
1. Introduction.....	1
A. Purpose	1
B. Scope and Methodology.....	1
C. Background.....	1
2. Results of Audit.....	3
A. System Security Configurations.....	3
B. Automated Information Systems Developments.....	11
C. Disaster Recovery and Continuity of Operations Plans.....	14
D. Segregation of Duties and Change Management Process.....	16
E. System Facilities Physical Conditions.....	19
F. Isolated NT Network	25
G. Peer-to-Peer Technology	27
Table 1. Averages Based on Center for Internet Security Scores.....	5
Table 2. User Statistics.....	6
Table 3. Average Number of Days Since Users Last Password Change.....	6
Table 4. Average Number of Days Since Last Log On.....	6
Table 5. Physical Observation Summary.....	16
Appendix A. NMAI Security Configuration Comparison to Industry Standards	31
Appendix B. Electronic Data Archiving.....	32
Appendix C. Management Comments From W. Richard West, Director, NMAI	33
Appendix D. Management Comments From Dennis Shaw, Chief Information Officer.....	45

ABBREVIATIONS AND ACRONYMS

CRC	Cultural Resource Center
GAO	General Accounting Office
GGHC	George Gustav Heye Center
IM	Instant Messaging
IP	Internet Protocol
IT	Information Technology
NCC	Network Communication Center
NIST	National Institute of Standards and Technology
NMAI	National Museum of the American Indian
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
p2p	Peer-to-Peer
RITS	Registration Information Transaction System
SANS	System, Audit, Network, Security Institute
SD	Smithsonian Directive
SI	Smithsonian Institution
TRM	Technical Reference Model
UPS	Uninterruptible Power Supply

INTRODUCTION

A. Purpose

With the planned opening of the new Mall Museum approaching, National Museum of the American Indian (NMAI) recognized the need for improvements in the technology area. NMAI requested a comprehensive review and the Office of the Inspector General initiated an audit of NMAI information systems. The purpose of the audit was to evaluate NMAI information system controls for systems access, server and network security, application development and program change management and service continuity.

B. Scope and Methodology

The audit was conducted from July 1, 2002, to November 27, 2002, in accordance with generally accepted government auditing standards. The audit methodology consisted of the following:

- identifying and reviewing applicable policies and procedures related to system general controls, computer system security, and integrity of computer resources
- comparing NMAI's system security settings with industry and Smithsonian Institution (SI) standards
- evaluating controls to safeguard and protect networks
- assessing the adequacy of controls to prevent and detect unauthorized activities including external intrusions, theft, or misuse of computers and networks
- utilizing guidance issued by the National Institute of Standards and Technology, National Security Agency, and Microsoft Corporation relating to system security configuration, disaster recovery and business continuity planning

We reviewed:

- policies, procedures, and controls relating to system security and data integrity
- controls over server and network configurations
- application development practices
- controls to prevent and detect unauthorized activities

As part of our review, we conducted interviews with technology and systems developers, administrative staff and support contractors. We spoke with staff from Information and Technology Resources, the Registrar's group, Film and Video, Membership, and Development. We also spoke with consultants supporting the FARSIGHT and Registration Information Transaction System applications. Through interviews, we gained an understanding of the practices employed concerning system configuration, network analysis, system access, disaster recovery and business continuity, and change management.

C. Background

The National Museum of the American Indian seeks to advance knowledge and understanding of Native cultures and strives to protect, support, and enhance the development, maintenance, and perpetuation of Native culture and community. As it prepares to open its new Mall Museum at the end of 2004, NMAI's strategic plan helps highlight the importance of technology and information management as a priority.

In order to meet the objectives noted in its strategic plan, NMAI recognizes the importance of information system security planning and the need to protect information technology resources. Each objective outlined in the plan provides detailed steps for achieving NMAI's major goals. Furthermore, each of NMAI's major goals strives to support achievement in the overarching Smithsonian-wide goals of public impact; focused, first-class research; management excellence; and financial strength.

As part of our review, we identified four major goals that incorporate the need for information security planning. First, in order to manage a comprehensive program to open the Mall Museum by the end of 2004, NMAI plans to ensure timely and successful installation and testing of all electronic, technology, and information management systems.

Second, in order to preserve, protect, relocate, selectively expand, and provide access to NMAI collections, NMAI plans to install a collections database (objects, photos, paper) with user-friendly accessibility for researchers and other interested parties.

Third, in order to enhance and implement organizational and management practices, procedures, and systems, and adopt appropriate technologies to improve effectiveness, efficiency, and productivity, NMAI plans to identify NMAI-wide technology and information management priorities and associated costs. This would include identification of those baseline technology applications that are essential to facility and collections management, administrative support, communications, and collaboration with Native communities and other entities. The Museum recognizes that overall database management and design is an important part of this process.

Fourth, in order to recruit, retain, support, and reward staff to carry out NMAI's mission, NMAI plans to manage an active, supportive, and responsive human resources operation. It would include recruitment, training, implementation of disciplinary actions, time and attendance tracking, and maintenance of performance plans and appraisals. It would also establish clear performance targets and provide special training opportunities for NMAI staff to gain and expand knowledge and proficiency in key areas related to their individual work.

RESULTS OF AUDIT

A. System Security Configurations

System security configuration at NMAI is vulnerable and does not meet industry security standard recommendations. Specifically, operating system security patches¹ and hotfixes,² or technical solutions to system vulnerabilities, were not up to date and server configurations were not documented. This occurred because there are no policies, procedures, or guidelines within NMAI that provide instruction on system security configuration. Technical staffs training programs were undefined, information technology position descriptions did not address accountability for system security, and there was no process in place to perform scheduled server and network risk assessments. As a result, current system configurations permitted the setting of blank passwords, allowed unauthorized, undetected connections, and many system users had more system rights than necessary.

Background

We evaluated NMAI system security at locations in Suitland, Maryland, Washington, D.C. and New York [George Gustave Heye Center (GGHC) and the Bronx Research Branch]. We used Smithsonian Directives and industry guidance and standards from the National Institute of Technology and Standards, General Accounting Office, National Security Agency, and Microsoft Corporation. The evaluation included a review of operating system configurations, user accounts, network ports, and vulnerable services.³

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that shall apply to Institution units. In particular, the directive requires managers to take systematic and proactive actions to develop and implement appropriate, cost effective management controls. It also requires that controls established shall provide reasonable assurance that assets are safeguard against waste, loss, unauthorized use, and misappropriation.

Smithsonian Directive 931, *Use of Computers & Networks*, August 5, 2002, requires the protection of business communications from unauthorized access.

The *Computer Security Act of 1987* requires the establishment of minimum acceptable security practices related to federal computers. This act requires the identification and protection of systems containing sensitive information and calls for a computer standards program and security training for users.

National Security Agency (NSA) 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

¹ A service pack is a periodic upgrade to the operating system that contains vulnerability fixes.

² Hotfixes are updates addressing specific vulnerabilities and errors introduced between service packs.

³ Registry settings and Novell servers were not evaluated.

certain threats and also practical. A balance is necessary between security and operations because some controls impede operational capability.

NSA, *Guide to Securing Microsoft Windows NT Networks*, 2001, identifies a variety of available Windows NT 4.0 security mechanisms and provides steps or 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, additional add-on service packs, and hotfixes.

Microsoft White Paper, *Securing Windows NT Installation*, 1997, states the default, out-of-the-box NT configuration is unsecured. This white paper discusses various security issues with respect to configuring all Windows NT operating system products for a highly secure computing environment.

National Institute of Standards and Technology (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 responsibilities and expected behavior of all individuals who access the system.

NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001, states adequate security of information and the systems that process it is a fundamental management responsibility. This document provides guidance on applying a framework by identifying 17 control areas, such as those pertaining to identification and authentication, and contingency planning. The guide explains that officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. This self-assessment guide provides a method for agency officials to determine the current status of their information security program.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996, defines eight principles used as an anchor on which the federal community should base their information technology security program. These principles guide personnel when creating new systems, practices or policies. This guidance defines the purpose of computer security as a way to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, a security program helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

Result of Review

We evaluated system configurations that included server and sub-network security at each of the NMAI locations. Under the current system configuration, we determined that the systems are vulnerable and could be strengthened to meet industry security standard recommendations. We used the Center for Internet Security Scoring Tool as a basis to evaluate each Microsoft NT server. The tool produces a score by applying the "Windows Security Scoring Tool" which is a number between one and ten, with ten being the most secure. The criteria used for scoring are divided into four categories: (1) Service Packs and Hotfixes, (2) Policies, (3) Security Settings and (4) Available Services and Other System Requirements. NMAI falls in the low range of average scores with a score of 3.54. Table 1 summarizes the averages for hotfixes and server scores for each location.

Table 1. Averages Based on Center for Internet Security* Scores						
Location	DC	NCC	Registrar	GGHC	Bronx	NMAI
No. of missing hotfixes and security patches	19.33	6.00	11.00	10.50	12.33	11.83
Missing service pack	Some not Updated	Some not Updated	Some not Updated	Updated	Updated	
Score	2.53	4.40	3.15	3.80	3.8	3.54

The failure to maintain servers with the most current versions is a risk that can be easily mitigated. A service pack corrects known problems and provides tools, drivers, and updates that extend functionality and keep the software code updated. 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. According to the NIST, maintaining and updating applications with the latest hotfixes, patches, and service packs is necessary to maintain the operational availability, confidentiality, and integrity of information technology systems. Not all vulnerabilities have related patches, therefore, system administrators must be aware of vulnerabilities and patches, and have a means to mitigate "unpatched" vulnerabilities through other methods.

Our review of the server security settings determined that across NMAI, audit policies and account lockout were not fully activated. Activating and reviewing events from audit policies can inform administrators of actions that could pose security risks and also identify the user accounts from which audited actions were taken. Microsoft recommends auditing and recording particular failed log on attempts, attempts to access sensitive data, and changes to security settings. Only three of five servers in the New York area had the audit control function activated. The remainder of NMAI's servers did not.

The account lockout function prevents brute-force password cracking or guessing attacks on the system. When activated, system administrators can set the number of log on attempts and the locking duration. In addition, information technology staff had not activated system password policies specifying password lengths and expiration dates. Specifically, no NMAI servers had activated the built-in Windows NT password policies. However, 75 percent of the servers (9 of 12) had activated the expiring password function.

Table 2 shows that the 12 servers had 249 local users. There were 32 users with blank passwords and most administrative accounts were not renamed. The Guest accounts were inactivated but not renamed. Both NIST and NSA recommend renaming or disabling these accounts. See Appendix A for a comparison of NMAI to Industry configuration standards. Industry standards recommend that users should have limited access to only what they need in order to perform their duties. An analysis of NMAI users identified that there are 70 users that have never logged on and 84 users that belong to the administrator group. A user in the administrator group has unlimited and unrestricted access to alter and make changes to systems.

Table 2. User Statistics							
		Averages					
	Total Users	NMAI	DC	NCC	Registrar	GGHC	Bronx
Local users	249	20.27	37.00	27.50	5.50	22.00	9.33
Local users with admin privilege	84	6.57	11.67	2.50	2.00	10.00	6.67
Account that have never logged (excluded guest)	70	5.73	10.67	8.00	1.00	7.00	2.00
Users with anonymous access		15.00	15.00	15.00			
Guest users		2.90	3.67	1.00	2.50	4.00	3.33
Generic users or process		8.77	8.33	15.00	2.50	13.00	5.00
Blank password accounts	32						

Tables 3 and 4 show the administrator group average time since the last password change was 562.9 days and the average time since last logon was 290.37 days. In addition, all the users belong to the administrator group on two servers. A review of these users is necessary to validate the need to maintain the various users and their level of system access. System administrators have begun this review and have removed some users and group accounts.

Table 3. Average Number of Days since Users Last Password Change						
	NMAI	DC	NCC	Registrar	GGHC	Bronx
Administrators	562.90	529.33	540.00	673.50	433.00	638.67
Others	592.23	614.67	252.00	641.50	655.00	798.00

Table 4. Average Number of Days Since Last Log On						
	NMAI	DC	NCC	Registrar	GGHC	Bronx
Administrators	290.37	241.33	165.00	348.50	251.00	446.00
Others	210.70	227.00	128.00	454.50	136.00	108.00

As part of our network analysis, we performed network scans and limited penetration testing on the NMAI network. Specifically, we researched and used the most common identified port and service vulnerabilities for Windows operating system. We scanned the network from both within and outside of the SI network. Although we were unable to easily identify the NMAI servers from outside the SI network, we were able to compromise the NMAI network from within the SI network.

We performed port scanning and penetration testing to determine open and vulnerable ports across the network. We reviewed those machines identified as susceptible to hacking and focused on the servers and then on the client machines. We used the NSA report "Windows NT Security Guidelines," as a basis for evaluating server services. In summary, NSA provides the following recommendations in order to minimize service risks:

- limit the necessary services that run on a given computer
- eliminate or separate services that interact with one another when not necessary
- perform periodic reviews on each computer on the network
- block server operators that can expand their capabilities or install programs that run with full administrative capabilities (Such capabilities are contrary even to standard Windows *NT* settings.)
- permit only full administrators to install services.

We performed limited attempts to penetrate selected machines. We recognized that once one machine was compromised, the password file containing all users' passwords could be captured and subsequently used to try to gain access to other machines. This would create a domino effect across the entire network. From our testing of 379 NMAI machines, we were able to penetrate 32 machines and collect password files that contained the system administrator's accounts, which provided us with the ability to compromise other SI computers.

Based on our analysis, we determined that system security weaknesses stem from the following:

- a lack of policies and guidance for server and client security configuration
- undefined technical staff training programs
- information technology position descriptions that do not address accountability for system security
- no process to perform periodic server and network risk assessments.

Although the Institution is establishing enterprise computer security policies, there is no NMAI guidance currently in place to assist system administrators in establishing minimum server and client security configurations. The NIST special publication *Principles and Practices for Securing IT Systems*, contains 14 practices that define an effective computer security program. These practices include the guidance for server and client security configuration that would help NMAI establish goals and assign responsibilities to administrators and users for the protection of assets under their custody.

NMAI information technology staff informed us that they did not receive any significant information technology security training within the last 18 months. Although staff has been maintaining NMAI systems, NMAI would benefit from a defined technology-

training program that identifies the specific technical skills necessary to maintain its systems. In addition, individual information technology position descriptions do not address accountability for system security in which they are inherently responsible for administering and maintaining. According to numerous federal standards, defining and implementing technology training programs is critical to the successful administration of information system resources.

There is no process to perform scheduled server and network risk assessments. Such assessments would be helpful in the evaluation of the many types of changes that affect system security. They could include evaluating technological developments, intra-network and inter-network changes, changes in the value or use of information, or the emergence of a new threat.

As a result, the lack of standard security system configurations places NMAI system resources at risk for unauthorized, undetected activities. In addition, without documented maintenance and administration responsibilities, NMAI cannot ensure that their systems are maintained in an updated and secure condition.

Conclusion

Based upon our configuration and network analyses, we believe NMAI can improve systems security by defining security administration responsibilities and introducing an assessment process into their administration duties. According to federal requirements, information technology staff should participate in a structured training program that provides the level of technical skills appropriate to their responsibilities. In addition, implementing security monitoring tools and performing periodic network scans can limit risks and vulnerabilities and prevent system compromises.

Recommendations

We made six recommendations to the Director, National Museum of the American Indian.

1. Use technical industry guidance to develop and implement server and client configuration settings.

Management Comments

Agreed. Management has circulated technical industry guidance among staff. NMAI will hire a Technology Manager who will issue a series of directives and assume responsibility for on-going compliance. Additionally, management intends to limit administrator group privileges to include only necessary personnel.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in June 2003 to obtain the status of this recommendation.

2. Define technology positions and include a delegation of system security responsibilities.

Management Comments

Agreed. NMAI has begun a process to revise all technology-related positions and the duties assigned as part of a general reorganization of the Information and Technology Resources office. System security responsibilities will be written into position descriptions and performance measures.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in June 2004 to obtain the status of this recommendation.

3. Develop a tailored technical training program for technology staff.

Management Comments

Agreed. Management will work with OCIO to assess training needs and develop an on-going security training program.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in October 2003 to obtain the status of this recommendation.

4. Develop and implement a semiannual security assessment process for systems and network assets that includes server configuration evaluations and network scans based on industry standards.

Management Comments

Agreed. NMAI staff will apply the *Windows Security Scoring Tool* on a quarterly basis and NMAI's Technology Manager will monitor compliance.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in March 2003 to obtain the status of this recommendation.

5. Review and determine the necessity of the numerous user accounts.

Management Comments

Agreed. NMAI system administrators will review and delete unnecessary accounts.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in January 2003 to obtain the status of this recommendation.

6. Review the current system configurations and make adjustments where necessary to enhance system security.

Management Comments

Agreed. NMAI's Information and Technology Resources Manager will oversee systems security configurations.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in April 2003 to obtain the status of this recommendation.

B. Automated Information Systems Developments

NMAI could benefit by following a system development life cycle methodology for its current application development projects. Until recently, the Institution did not have guidance to assist developers who develop application projects. Without a development methodology, NMAI projects could fail to meet project deadlines and budget requirements. In addition, without an adequate project plan, management oversight would be difficult.

Background

The scope of our review consisted of evaluating project management practices for its application development projects. We interviewed NMAI staff and reviewed documentation for current projects (Collection Information System, Media Information Management, Contact Management System) under development.

Smithsonian Directive 910, *Information Technology Planning*, August 28, 2002, establishes policies and procedures and assigns responsibilities for strategic and operational information technology planning within the Institution. Within each of their areas of responsibility, museums, research centers, and office directors will designate a person to conduct or coordinate IT planning activities and develop IT plans with guidance from the Chief Information Officer.

Smithsonian Directive 920, *Life Cycle Management*, August 5, 2002, establishes life cycle management policies, defines essential elements, and assigns responsibilities governing the initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement of automated information systems and IT infrastructure projects at the Smithsonian Institution. In addition, the directive requires logical planning, managing, and monitoring of automated information system developments. Each development phase requires specific decisions and actions, to ensure that the system is being developed and managed efficiently, economically, and that it meets requirements.

Result of Review

In performing our review, we determined that the Museum is in the midst of developing major application projects. Based upon our evaluation, NMAI could benefit by following a system development life cycle methodology for its current application development projects. Reviews of application development documents and discussions with NMAI development staff determined that no formal development methodology was followed. In addition, there were no written preliminary project plans or a business case, as required by the current life cycle management policy. However, the available technical documentation for the collections and media information projects was detailed. Both Smithsonian Directives 910 and 920 establish requirements for defining the bases, scope, and possible improvements for any project. According to the policies, a well-defined project plan needs to be in place. Additionally, application projects must be supported by a business case that includes an analysis of the expected costs and benefits, alternative solutions, and potential programmatic and technical risks. No application development project should be initiated until supported processes have been reviewed and redesigned as necessary for their greatest possible effectiveness.

Until recently, the Institution did not have detailed guidance and policies for technology staff to follow regarding system development projects. Directives 910 and 920 issued in August 2002 should strengthen the Institution's ability to consistently develop and implement information systems. NMAI's developer did state that since SI has two new directives, NMAI plans to follow SI policy when developing and implementing application projects.

Employing and following a structured system development methodology would assist in maintaining a project focus and identifying critical paths and development issues before funds are spent and milestone dates approach or pass. Without project plans, NMAI projects could fail to comply with deadlines and budget requirements. In addition, without an adequate project plan, management oversight is difficult. Without a defined development life cycle, projects become too complex to plan and control successfully.

Conclusion

The Museum has established within its 2002 strategic plan, goals to enhance and implement organizational management practices, procedures and systems, adopting appropriate technologies and other methods to improve effectiveness, efficiency, and productivity. We believe that the adoption of such a structured development methodology for all development applications, regardless of size, would benefit NMAI strategic goals.

Recommendations

We made two recommendations to the Director, National Museum of the American Indian:

1. Define an NMAI sponsor and formally define a development implementation team for the collection management system, media information management, and contact management system.

Management Comments

Agreed. NMAI's Collections Information System development implementation team will be established in February 2003. The Media Information Management System development implementation team will be established in June 2003, and the Contact Management System development implementation team will be established in February 2003.

Office of the Inspector General Response

The Director's actions are partially responsive to the recommendation. The recommendation called for NMAI to assign a sponsor within NMAI to be responsible for the programs being developed. We request that NMAI identify a unit to sponsor and have responsibility for overseeing and implementing each program. We will follow up with the Director in June 2003 to obtain the status of the three systems indicated this recommendation.

2. Require that current and future development projects follow the SI life cycle management policy.

Management Comments

Agreed. NMAI's Technology Manager has instructed staff to follow recently issued institutional guidance provided by *Technical Standard & Guideline IT-920-01 Life Cycle Management Manual*.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. This recommendation is considered closed.

C. Disaster Recovery and Continuity of Operations Plan

Although a tape backup process is in place, NMAI had not implemented a disaster recovery and continuity of operations plan for IT services. A disaster recovery and continuity plan had not been initiated because NMAI is awaiting OCIO guidance for standardizing sensitivity and risk assessments documentation required for Institution-wide planning. In addition, funding has been budgeted for fiscal year 2003 to assist in implementing security plans for major system development projects. Without fully implementing these plans, the Museum may not be prepared in the event operations are disrupted due to system failure, compromise, or other disaster.

Background

The scope of our review consisted of evaluating NMAI's existing disaster recovery and business continuity plans for system resources. We interviewed NMAI management and information technology staff to gain an understanding of backup and disaster recovery and continuity of operations plans.

Smithsonian Directive 931, *Use of Computers & Networks*, August 5, 2002, requires system administrators to perform data back up and offsite storage of critical data. In addition, *Smithsonian Institution Computer Security Handbook*, September 9, 1993, provides computer security policies and procedures for all Smithsonian components to develop disaster recovery and business continuity plans. Disaster recovery safeguards consist of developing a contingency plan, storing the plan offsite, regularly backing up files and software, identifying an alternate offsite processing site, and testing the contingency plan. According to the Handbook, the purposes of a contingency plan are to determine actions that will minimize the effects of undesirable occurrences, document emergency response actions like system restart, and establish procedures for recovering from losses.

NIST, *The Contingency Planning Guide for Information Technology Systems* December 2001, provides instructions, recommendations, and considerations for government IT contingency planning. According to the guidance, some type of documented procedures should be in place to provide for the recovery of files, address disaster recovery, and identify critical processing data. The plan should allow for periodic testing and should ensure that personnel understand their respective roles during a disaster.

Results of Review

Our review determined that NMAI has not documented or implemented disaster recovery business continuity of operations plans that cover its system resources. Disaster recovery and contingency plans assess the adequacy and ensure continuity of operations if either a complete system failure or failure of system components occurs. For its system servers, system administrators have an established tape backup process. The tapes, however, are not stored off site at all locations.

Disaster recovery and continuity of operations planning for critical systems is a top priority for management. Although, technology staffs have identified processes in the event of a short-term disruption, management has not taken steps to develop and implement full disaster recovery and continuity of operations plans because they are awaiting institution guidance from the OCIO. The OCIO is planning on establishing

policies and guidance for disaster and continuity planning in the near future. In anticipation of the need for disaster recovery and continuity planning, the Museum has included funding in its fiscal year 2003 budget for obtaining contract support to assist in performing sensitivity and risk analyses for major systems.

Without a plan in place, NMAI risks the ability to restore its critical system resources in a timely manner if one of its components fails due to an unforeseen situation. In addition, without these plans, the opening of the new Mall Museum could face disruptions that could not be addressed in a timely manner.

Conclusion

With the planned opening of the Mall Museum, it is critical that plans are in place to address any level of system disruption. The top NMAI goal is to manage a comprehensive program to construct and open the Mall Museum by the end of calendar year 2004. One of NMAI's objectives is to ensure timely and successful installation and testing of all electronic, technology, and information management systems necessary for effective operations, and for linkages with other NMAI operations. Without a disaster recovery and continuity of operations plan, achievement of NMAI strategic goals is at risk.

In addition, the Museum has an opportunity to consider electronic data archiving between its three facilities (Manhattan, Suitland, and the new museum opening in the District) for its disaster recovery continuity of operations. Data archiving provides numerous benefits in both cost and operations. Appendix B illustrates an example of electronic data archiving between the three locations. The advantage of electronic data archiving, or auto archiving as it is sometimes called, is the ability to store offsite without the extra expense of a hotsite facility. Another advantage of auto archiving is the ability to quickly restore a system, which increases the amount of system space availability.

Recommendation

We recommended that the Director, National Museum of the American Indian, adopt and implement a disaster recovery and continuity of operations plan in accordance with SI policies or current industry standards.

Management Comments

Agreed. NMAI's new Technology Manager will oversee the development of an NMAI Disaster Recovery and Contingency Plan and the Information and Technology Resources Manager will oversee implementation of disaster recovery plans.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. The Chief Information Officer issued guidance for conducting sensitivity analyses and risk assessments on November 5, 2002, as a result, assessments can begin at any time. We will follow up with the Director in July 2003 to obtain the status of this recommendation.

IT-930-01

} See PRISM

D. Segregation of Duties and Change Management Process

Currently, there is inadequate segregation of duties for the administration of the financial application FARSIGHT. In addition, the Museum has not adopted a system change management process for FARSIGHT. This is occurring because application administration is being supported outside of the Museum's technology staff. As a result, inadequate segregation of duties increases the risk that erroneous or improper program changes could be implemented and that the computer resources could be damaged or destroyed.

Background

The scope of our review consisted of evaluating the change management process for the FARSIGHT application. We interviewed NMAI staff, the contracting officer's technical representative, and the contractor responsible for the application.

General Accounting Office (GAO), *Federal Information System Audit Controls Manual*, January 1999, requires that segregation of work responsibilities occur so that no individual controls all critical stages of a process. It also restricts the designated computer programmer from independently writing, testing, and approving program changes. The manual states that inadequately segregated duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and the computer resources could be damaged or destroyed.

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that shall apply to Institution units. In particular, the directive requires managers to take systematic and proactive actions to develop and implement appropriate, cost effective management controls. It also requires that controls established shall provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

Results of Review

As part of our testing of general access controls, we determined that NMAI has contracted for server and FARSIGHT application administration that includes making program change and modifications. FARSIGHT is an application used by 99 users that contains financial budget and obligations information concerning NMAI projects and salary forecasting. Typically, separation should exist among individuals who maintain the applications, individuals who administer the application server, and individuals who make application changes and modifications. Discussions with the FARSIGHT support contractor revealed that the contractor performs server administration, application modifications, testing, and implementation. Further, NMAI is not requiring technical documentation that explains the application changes or the maintenance of documented correspondences and requests for changes between the contractor and the contracting officer's technical representative. In addition, NMAI is providing the contractor with two computers for their use. These computers and the application server are located in a public space to ease system administration.

Reliance on a contractor for performance of all of these duties without proper oversight by technically trained staff is a risk. Responsibilities of the contracting officer's technical

representative include representing the Smithsonian in issues with the contractor, including acceptability of workmanship, compliance with technical requirements of the contract, completion of work, and approval for payment. The contracting officer's technical representative supporting NMAI's FARSIGHT application is not trained in information technology and not familiar with the segregation of duty responsibilities. Delegating technical oversight to non-technical staff without adequate training and experience poses a risk to the Museum.

As a result, it would be difficult for the current contracting officer's technical representative to effectively question the work of a technical contractor. In addition, unnecessary software changes could be implemented due to a lack of effective controls to segregate duties and monitor contract performance. Also, permitting unnecessary computer access and resources poses a risk of improper use of computer resources within NMAI and the Institution.

Conclusion

One of the Museum's strategic goals is to enhance and implement organizational and management practices, procedures, and systems at NMAI and adopt appropriate technologies to improve the effectiveness, efficiency, and productivity. If staff is unfamiliar with the Institution's standardization of technologies and oversight, they risk supporting an ill-advised application or an application that is not a standard. Such applications could pose additional vulnerabilities and risks.

Recommendations

We made four recommendations to the Director, National Museum of the American Indian:

1. Assign contract oversight responsibilities for technical contracts to qualified information technology staff.

Management Comments

Agreed. NMAI's Information and Technology Resources staff will work closely with the Contracting Officer's Technical Representatives managing technical projects to provide contract oversight for technical issues. Information and Technology Resources staff will apply Life Cycle Management guidelines to legacy systems.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. Although not explicitly stated by NMAI, we believe that NMAI should have IT staff involved on its current technical contracts. We request that NMAI clarify whether this is their intent and we will also follow up with the Director in June 2003 to obtain the status of this recommendation.

2. Define and implement, with support from the Office of Contracting, a contract modification for the maintenance of system support technology contracts.

Management Comments

Agreed. NMAI will review the existing contract for the FARSIGHT vendor and, with support from the Office of Contracting, specify systems maintenance requirements.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in April 2003 to obtain the status of this recommendation.

3. Obtain the system documentation, including changes, from the FARSIGHT contractor and establish a change and configuration management process for future modifications.

Management Comments

Agreed. Systems documentation will be requested immediately and a change and configuration management process will be established.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in April 2003 to obtain the status of this recommendation.

4. Perform an information technology organization assessment to include considering realigning technology positions under a central manager.

Management Comments

Agreed. NMAI will present a draft proposal to assess information technology organization and realign technology positions under a central manager to Senior Management and its Board of Trustees.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in June 2003 to obtain the status of this recommendation.

E. System Facilities Physical Conditions

Physical computer security conditions at NMAI can be improved. Currently, physical access, fire prevention, air-cooling, plumbing, and housekeeping conditions pose a risk to system resources and staff. This is occurring because SI has not issued computer room physical condition policies and NMAI has not obtained budgetary support to enhance its facilities. In addition, for convenience, NMAI maintains its computer rooms accessible to non-technology staff. Without appropriate physical and environmental security controls implemented to protect the system resources, the system resources themselves, are at risk for unauthorized changes to hardware or software configuration. They are also at risk for theft. In addition, without strict computer room housekeeping requirements, there is a risk of fire and accidental damage to equipment.

Background

We visited each location to obtain a first hand observation and understanding of the physical security current conditions. The scope of our review consisted of evaluating physical access controls, fire hazards, utilities, and housekeeping risks to computer resources.

SI Directive 115, *Management Controls*, July 1996, establishes that management controls must provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation. Access to resources and records should be limited to authorized individuals and accountability for the custody and use of resources should be assigned and maintained.

GAO, *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.

The 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 NIST guidance, 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.

The NIST special publication 800-18, *Guide for Information Technology Systems*, December 1998, states that physical access controls should be in place to restrict the entry and exit of personnel from a data center area or room containing network equipment. Physical access controls should address not only the area containing system hardware, but also the wiring, and the uninterruptible power and backup operations that support system operations.

Results of Review

In performing our review, we determined that the physical conditions surrounding NMAI's computing resources can be improved. Table 5 shows a summary of our physical observations for each location visited.

Table 5. Physical Observation Summary				
	CRC	DC	NY	
			GGHC	The Bronx
Physical Access Control				
Public access to computer resources	X	X	X	X
Fire Safety Factors				
Fire suppression prevention devices installed and working	X	X	X	X
No emergency water cutoff	X	X	X	X
Supporting Utilities				
Building plumbing lines are known to endanger systems			X	X
No uninterruptible power supply	X	X	X	X
Unkempt housekeeping			X	X
X = location is not to standard.				

At CRC, we observed that although the door to the Network Communication Center (NCC) room has an electronic lock, it is not used. Also, we observed that the room is left unattended and this provides opportunities for someone to enter and alter or damage servers and network equipment. In the New York GGHC facility, the room is accessible with a key card; however, it is shared with the Film and Video Center. Staff also uses the space to store their bicycles and other equipment. Additionally, a makeshift office is established for a support contractor, generating traffic unrelated to the servers' administration. Further, the servers are located inside a cage that is open at the top.

In the Bronx, the computer room door can be opened with a general key and a network router is located in an open, unsecured public area next to oily mechanical machinery. In the Washington, D.C. facilities, the server that maintains financial data is located in an open, public area. Another server is on top of a file cabinet in a storage room accessible by others. The servers are also publicly accessible with a general key.

In all locations, we observed that fire suppression and some supporting utilities were not fully in place. For example, although most locations rely on water sprinkling systems, there are no emergency water cut-offs. Because most of the system resources are stored in general building space, there are no backup and auxiliary cooling systems in place. As a result, we noted the locations that housed the server resources were warmer than the remainder of the building.

The two locations in New York pose a significant plumbing risk. In the GGHC facility, pipes run along the ceiling above the servers and in the Bronx, the server room is located between two bathrooms, and the room has an open hole in its ceiling. Also, the

equipment is not protected in case of electric shut off and there is no uninterruptible power supply (UPS) or no backup generator. NMAI staff stated that they contacted the local facilities office regarding this problem. In regards to housekeeping conditions, we noticed that the GGHC computer room contained trash paper and soft drink cans. Such conditions pose fire and safety hazards and the potential risk of damage to equipment.

In general, these conditions exist because focus has been on the opening of the new Mall Museum and because of budget and space constraints. Also, the SI does not have detailed policies that address computer room physical conditions. The OCIO is in the process of formulating SI policy for computer room physical conditions.

At both the D.C. and CRC locations, the computer rooms are left open to all staff for convenience purposes. CRC staff explained that the door to the computer room is open because staff need access to a high quality copier used for graphic copying. In the D.C. location, the computer servers are placed in publicly accessed locations because a contractor requires access to perform administration on the FARSIGHT application. Another server is located in a storage room on top of a file cabinet, but according to staff, plans exist to relocate this server to OCIO. Other computer servers, however, were secured from public access. The GGHC staff explained that the computer room is publicly accessible because, historically, several different offices, including Film and Video Center, used it. The Bronx server computers are accessible because the lock to the server room door can be opened with the building front door key. The front door keys can be obtained from any Bronx facility staff person.

At all locations, although fire sprinklers were visible, hand held fire extinguishers were not. We believe that the lack of SI policies for computer rooms contributes to staff failure to maintain additional fire suppression needs. In addition, GGHC staff failure to maintain general housekeeping is due to the difficulty of management to provide oversight from a distant location (the CRC) and a lack of SI policy or standards.

Funding and upgrading for the D.C. facility is not planned because resources will be directed to the new Mall Museum building. At the GGHC, staff stated that UPS has been requested but not received. In addition, staff stated that requests were made to the General Services Administration who manages the facility, to assist in determining an alternative means for backup power supply. Also, at the GGHC, there are visible ceiling plumbing pipes with no protection to the computers below. Staff stated that with OCIO involvement, plans are being made to consolidate several SI museums computer resources in the New York area at the GGHC. It is unclear whether the new plans will address the plumbing issue because at the time of our audit, formal plans were incomplete.

A lack of physical and environmental access controls increases the risk to computer resources. Individuals can gain unauthorized access to terminals or telecommunication equipment that provide access to confidential or sensitive information, substitute unauthorized data or programs, and steal or inflict malicious damage to computer resources. In addition, without strict housekeeping requirements, there is a risk of fire and accidental damage to equipment and staff.

Conclusion

Current industry standards recommend following a "least privilege" access methodology whereby individuals are limited to system access. Access is granted only to the resources needed to perform duties. Employing different locks at physical entry points and terminal locks on computers and relocating public resources from computer rooms are methods used to limit access.

Recommendations

We made nine recommendations to the Director, National Museum of the American Indian:

1. Relocate the copiers from the computer rooms and relocate the routers and servers from publicly accessible locations.

Management Comments

Agreed. NMAI plans to relocate the copier from the Network Control Center at the CRC to a different location. NMAI will also secure the router at the Research Branch and consider relocation of the servers for RAISER'S EDGE and FARSIGHT.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in May 2003 to obtain the status of this recommendation.

2. Examine staff access needs and storage requirements at the GGHC computer room and develop controls to prevent public access to the system resources.

Management Comments

Agreed. NMAI will relocate the video-conferencing equipment and the Film and Video Contractor.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in May 2003 to obtain the status of this recommendation.

3. Permit the GGHC computer facilities to be used only for maintaining computer resources.

Management Comments

Agreed. NMAI will reorganize staff to permit the GGHC computer facilities to be used only for maintaining computing resources.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in May 2003 to obtain the status of this recommendation.

4. Establish a separate lock and key at the Bronx location and identify appropriate staff to maintain the key.

Management Comments

Agreed. GGHC Security will install a new lock cylinder at the Research Branch and identify appropriate staff to maintain the key.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in January 2003 to obtain the status of this recommendation.

5. Install hand held extinguishers in computer rooms.

Management Comments

Agreed. Technology staff persons are researching appropriate hand-held fire extinguishers for NMAI's computer rooms.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in January 2003 to obtain the status of this recommendation.

6. While awaiting SI policies on computer rooms, issue guidance to staff on the need to maintain a safe working environment and reinforce more oversight of computer rooms.

Management Comments

Agreed. NMAI's Information and Technology Resources Manager will speak with staff and issue written guidance on the need to maintain a safe working environment.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in January 2003 to obtain the status of this recommendation.

7. Implement a backup and emergency power supply to secure NMAI system resources.

Management Comments

Agreed. NMAI is determining whether the GSA back-up generator can be used by NMAI. If this generator does not become available, NMAI plans to install additional uninterruptible power supply at the GGHC facility.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in June 2003 to obtain the status of this recommendation.

8. Complete the necessary additions to the GGHC computer room and assess the overhead plumbing situation.

Management Comments

Agreed. Once storage and staffing decisions are made, the necessary additions to the GGHC computer room will be undertaken. The Information and Technology Resources Manager will require plastic sheets to be available to drape over machines.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in July 2003 to obtain the status of this recommendation.

9. Establish procedures and persons responsible for maintaining proper housekeeping.

Management Comments

Agreed. NMAI's Information and Technology Resources Manager will establish procedures and task staff with responsibility for maintaining proper housekeeping.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in January 2003 to obtain the status of this recommendation.

F. Isolated NT Network

NMAI is unnecessarily operating a Windows NT network to support 25 Registrar staff. A former employee established the network and NMAI maintains it because they believe it is necessary to support the New York collections move database. Operating a separate network that is not consistent with the Institution's enterprise network, however, increases contractor costs in server administration and desktop support. NMAI and OCIO staff would otherwise perform this additional administration. In addition, there is a risk of internal NT network vulnerabilities.

Background

We interviewed NMAI Network Communication Center (NCC) administrators, Registrar administrators, and the Registration Information Transaction System (RITS) database developer contractor.

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that shall apply to Institution units. In particular, the directive requires managers to take systematic and proactive actions to develop and implement appropriate, cost effective management controls. It also requires that controls established shall provide reasonable assurance that assets are safeguarded against waste, loss, unauthorized use, and misappropriation.

Smithsonian Institution, Technical Reference Model (TRM), Version 1.0, December 2001, IT-920-01, applies to program area and technical managers, and others responsible for information technology systems and services. Compliance is required unless specifically waived by the Chief Information Officer. The TRM recognizes that the Institution is composed of varied and incompatible hardware and software. The heterogeneous nature of the institution's technology infrastructure has constrained its ability to infuse new technology. The TRM attempts to apply an enterprise approach to managing technology infrastructure. A more homogenous, standards-based, information technology infrastructure will provide the foundation for distributed systems, which are robust and scalable. The TRM attempts to establish consistent information and communication services throughout the Institution. A standards approach will provide the ability to update and replace technology in a more cost effective means. The TRM identifies Novell Netware as the preferred network operating standard.

Results of Review

Through our network analyses and interviews with technology staff, NMAI is unnecessarily operating a Windows NT network to support 25 Registrar staff. The Institution's enterprise network is Novell. For this reason, duplicate administration, outside of the Novell administration is required. The Registrar uses a support contractor to assist in maintaining the separate Windows NT network.

According to Registrar staff, a former Registrar staff member established the Windows NT network. The network was maintained under the premise that NCC staff members were not sufficiently experienced to administer the Registrar's needs and that the New York collections move required a Windows NT network to operate the RITS database. Based on our server and network evaluations, however, we determined that NCC staff had

administered similar system resources, and according to the RITS developing contractor, Windows NT network is not required for operating the RITS database. Both the RITS developers and the network administrator stated that the users could access the application through Novell. In fact, according to the RITS developers, currently, there are Novell users from Photography, Exhibition, and Curatorial who are accessing RITS. RITS was developed using Microsoft technology. Technically, only this Microsoft application needs to be maintained in the Microsoft environment. Users remain independent and may access the application from a Novell network.

Any unit that operates a separate network that is inconsistent with the Institution's enterprise network increases contractor support costs in server administration and desktop support. This additional contracted support otherwise would be performed by NMAI, NCC, and OCIO staff. In addition, there is a risk of internal denial of service attacks and data compromises due to the NT server vulnerabilities.

Conclusion

Standardization also has economic benefits because such unnecessary administrative funding can be put to better use. Also, following the SI technical model encourages standardization across the Institution.

Recommendation

We recommended that the Director, National Museum of the American Indian, eliminate the Windows NT network.

Management Comments

Agreed. The Information and Technology Resources Manager will request contract support to migrate the Registration Information Tracking (RITS) application to be accessible through the Novell network.

Office of the Inspector General Response

The Director's actions are partially responsive to the recommendations. We request clarification on whether the Director plans to eliminate the NT network and if not provide a technical justification to maintain its existence.

G. Peer-to-Peer Technology

Use of peer-to-peer technology (p2p⁴) puts NMAI systems and the SI network at risk. We found that staff was using p2p programs such as instant messaging and Internet file sharing programs. They were using instant messaging as a solution to communicate and file sharing programs for personal downloading of music and video. As a result, NMAI and SI system resources are vulnerable to viruses, worms, and denial of service attacks.

Background

The scope of our review consisted of evaluating the general software controls. We reviewed system server applications and client side applications and interviewed management and information technology staff.

Smithsonian Directive 931, *Use of Computers & Networks*, August 5, 2002, requires that the Institution's computers and networks be used only for Smithsonian related work. The Directive further states that Smithsonian communications must be protected from unauthorized access and that sensitive information including electronic mail and file transfers must be encrypted. The Directive lists different types of computer and network misuses that include seeking, transmitting, and storing offensive material. It states that copyrighted and licensed materials should not be used on a personal computer, SI Net, or the Internet unless legally owned or otherwise in compliance with intellectual property laws. Also, it states that each user should not overtax processing and storage capabilities by minimizing transferring audio and video files. Finally, it grants system administrators authority to access electronic files for system maintenance or development, system security, and correcting software problems.

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that shall apply to Institution units. In particular, the directive requires managers to take systematic and proactive steps to develop and implement appropriate, cost effective management controls. It also requires that controls established shall provide reasonable assurance that assets are safeguard against waste, loss, unauthorized use, and misappropriation.

System, Audit, Network, Security Institute (SANS), *Peer-to-Peer Networking*, October 29, 2001, concludes that the use of p2p software is a credible threat to network security. In addition, the limited documentation surrounding the technology hinders the capability of network and system administrators to analyze and obtain knowledge of vulnerabilities associated with its use. Often system administrators are unaware that users have downloaded and installed these applications. This lack of awareness renders system administrators incapable of protecting systems from the many p2p security loopholes. SANS notes the following problems with p2p technology:

- unnecessary network bandwidth utilization that congests networks
- illegal transfers that involve copyrighted material
- information leakage and loss of control over the data on computers and networks
- virus and Trojan propagation downloaded from untrusted sites.

⁴ According to the SANS Institute, p2p technology is a communication model in which each computer has the ability to initiate a communication session with other computers running p2p software. P2p applications enable users to use the Internet to exchange files and communicate.

- internet protocol and machine name disclosure outside the internal trusted network and firewall circumvention

Results of Review

NMAI used two p2p technology applications: instant messaging and file sharing. Our reviews identified *Instant Messaging* (IM) located on the server. Through network scans, we identified open ports commonly used by file sharing applications. There are currently four main IM products available for free. *AOL Instant Messenger (AIM)*, *ICQ Instant Messenger*, *Yahoo Messenger*, and *MSN Messenger Service* are programs that allow anyone to determine when users are online and available for messaging, chatting, or file sharing. IM programs do not provide the option of restricting others to add their names to their individual lists⁵. Some IM programs permit users to share entire file directories. Our identification of Kazaa, an Internet file sharing program within the NMAI network, also opens other vulnerabilities similar to the use of IM. Prior to our discovery of Kazaa, NMAI management notified staff that the museum and the Institution does not condone the use of p2p file sharing programs such as Napster, Kazaa, and Gnutella, all well known Internet file sharing programs.

NMAI information technology staff was using IM as a convenient communication method. During our audit, technology staff removed instant messaging from the server. Staff used file sharing programs for personal downloading of music and video. Additionally, NMAI technology staff and the computer security industry have all recognized that it is extremely difficult to identify and monitor the use of IM and file sharing programs within an enterprise network.⁶

As a result, according to Internet and computer security organizations, p2p technologies contain numerous documented risks. For example, privacy issues arise when personal and workplace information such as machine names and computers Internet Protocol (IP) addresses are disclosed. Unless an enterprise encryption program is put in place, all IM sent and received are transferred in plain text and susceptible to interception. Further, file transfers could allow infected files to bypass conventional antivirus protection. Although network gateway antiviral products can limit the transfer of malware⁷ files, these products must be strategically placed on the network and could interfere with network performance.

These well known file sharing programs pose a risk. Because shared files are commonly video and music files, which are extremely large in size as compared to normal network file traffic, they congest network links and unnecessarily occupy bandwidth required for official network traffic. Also, storage of large files has the potential to fill up hard drive and network file storage. It is well known that file sharing applications and their use provide a conduit for malware to circumvent firewalls and enter networks because almost all the sources of downloads originate from untrusted sources. The file sharing programs

⁵ Other users can determine when someone is online as long as they are included in their "buddies" list of contacts. There is no means to restrict someone from being added to someone else's "buddies" list.

⁶ Systems, Audit, Network Security (SANS) Institute, *The Instant Messaging Menace: Security Problems in the Enterprise and Some Solutions*, January 31, 2002, has identified instant messaging and p2p technology as a security threat to enterprise networks.

⁷ Malware is malicious code inserted or concealed in legitimate files. Computer viruses and worms are common malware code.

themselves often have hidden or backdoors built into them that permit outside users to enter and view files. Additional risks include copyright infringements and viruses and Trojan Horse program propagation.

Conclusion

Although specifically discovered during this audit, the use of p2p technologies, in all likelihood, is prevalent across the Institution. Because of the significant risks involved with p2p technologies, industry computer security experts have devised some remedies for enterprise networks. For example, industry experts recommend deploying an intrusion detection system to recognize pattern matching as an alert of large files transfers to identify potential file sharing activities. In addition, clear and accountable policies give notice to system users about the dangers and bandwidth disadvantages associated with the use of this technology.

Recommendations

We made two recommendations to the Chief Information Officer:

1. Issue policies and guidance on the use of p2p technology for the Institution.

Management Comments

Agreed. The Chief Information Officer plans to analyze safeguards for peer-to-peer technologies including instant messaging. The CIO plans to issue policies and guidance by July 2003.

Office of the Inspector General Response

The CIO's actions are responsive to the recommendation. We will follow up with the Director in July 2003 to obtain the status of this recommendation.

2. Modify the SI network control points to identify large file transfers and potential file sharing activities in order to alert network administrators.

Management Comments

Agreed. The CIO plans to upgrade the software in SInet routers by October 2003. These upgrades will allow the routers to recognize and restrict file sharing network activities.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in October 2003 to obtain the status of this recommendation.

3. We recommended that the Director, National Museum of the American Indian, perform periodic network and PC reviews to determine if p2p programs are being used and take appropriate administrative action when necessary.

Management Comments

Agreed. NMAI's Information and Technology Resources Manager will issue guidance about the use of p2p software and ensure periodic reviews check for misuse of p2p technology.

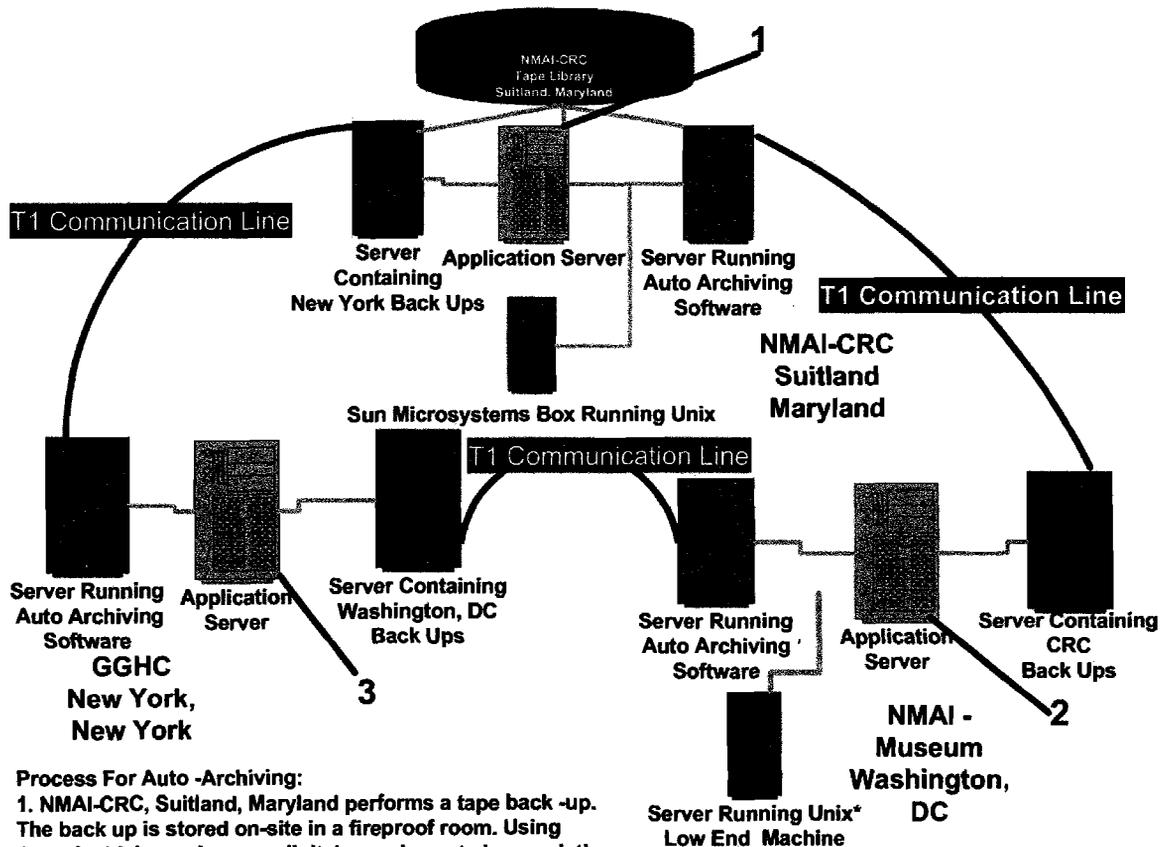
Office of the Inspector General Response

The Director's actions are responsive to the recommendation. We will follow up with the Director in March 2003 to obtain the status of this recommendation.

Appendix A. NMAI Server Security Configurations Compared to Industry Standards

Password Policy	CRC-CITRIX	CRC-BACKUP	NMAI-CRC-NTZ	CRC-SQL	Never expires	42 days	42 days	42 days	42 days	Never expires	NMAI-FAR	NMAI-RE	CITRIX_SERVER
Maximum password age	90 days	42 days	42 days	42 days	Never expires	42 days	42 days	42 days	42 days	Never expires	42 days	42 days	42 days
Minimum password age	1 day	Allow changes immediately											
Minimum password length	12 characters	Permit blank passwords											
Passwords Uniqueness (password history)	24 passwords	Do not keep password history											
Account lockout Policy	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout	No account lockout
Account Lockout	3 bad attempts												
Reset account after	15 minutes												
Lockout duration	15 minutes												
Forcibly Disconnect remote users when logon hours expire	Users must logon to change password												
force users off	select option												
Do Not Audit													
Audit These Events													
Logon and Logoff	Success, Failure				Success, Failure					Success, Failure			
File and Object Access	Failure				Success, Failure					Failure			
Use of User Rights	Failure				Success, Failure					Failure			
User and Group Management	Success, Failure				Success, Failure					Success, Failure			
Security Policy Changes	Success, Failure				Success, Failure					Success, Failure			
Restart, Shutdown, and System Process Tracking	Success, Failure				Success, Failure					Success, Failure			
No auditing	No auditing				No auditing					No auditing			

Appendix B. Electronic Data Archiving



Process For Auto -Archiving:

1. NMAI-CRC, Suitland, Maryland performs a tape back -up. The back up is stored on-site in a fireproof room. Using Auto-Archiving software a digital copy is sent via an existing digital connection to location 2(NMAI, Washington, DC)
2. NMAI Washington, DC receives a digital copy of NMAI-CRC back up. This back up is sent to the tape drive on the server, which received the digital copy of the back up. This copy is then stored on site at NMAI, Washington,DC. On another NMAI-Washington,DC server the daily back up of NMAI-Washington is being backed up to tape, after the back up has completed a digital copy of NMAI-Washington is sent to location 3(NMAI-GGHC in New York City) via an existing digital connection.
- 3.NMAI-GGHC receives the digital copy of NMAI Washington, DC back up as well as NMAI CRC back up, both back up are sent to the tape drives and a separate copy of both back up is made and stored on site at NMAI-GGHC. A back up of NMAI-GGHC is backed up on tape and then a digital copy of NMAI-GGHC is sent to NMAI-CRC via an existing digital connection. The digital copy of NMAI-GGHC is received at NMAI-CRC and backed up to tape and stored on site at NMAI-CRC. A digital copy of this back up from NMAI-GGHC is sent to NMAI-Washington, DC along with the digital back up of NMAI CRC. Using this suggested model NMAI would have a back up copy of all of their critical data stored at three different locations in case of a disaster which destroyed or disabled one of the NMAI facilities.

Memo

Date **January 6, 2003**

To **Thomas D. Blair**

cc **Dennis Shaw, Doug Evelyn, Jane Sledge**

From **W. Richard West**

Subject **Comments on Draft Report on Audit of Information System Controls at the National Museum of the American Indian**

Thank you very much for the opportunity to comment on the Draft Report. Please find our written comments attached to this memorandum.

I consider information and technology security to be an important part of good management practice and this survey is especially timely as we prepare for the opening of NMAI's new museum on the National Mall.

I very much appreciate this comprehensive review of our information security program and your staff's efforts and assistance. Let me express NMAI's sincere appreciation for the timely and constructive manner of this review and knowledge and experience your staff shared with us. We value your recommendations and take them seriously. The facts presented in the report are accurate, I concur with all the recommendations, and I present an action plan for implementation in the attached document.

Attachment

A. System Security Configurations

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. Use technical industry guidance to develop and implement server and client configuration settings.	Concur	The Information and Technology Resources (ITR) Manager, Jane Sledge, circulated the System Security Configuration Summary and Results prepared by the Inspector General's representative, David Cole, to technology staff and requested staff to review and update security settings vulnerabilities noted in the document.	Fall 2002
		The ITR Manager will work with a soon to be hired Technology Manager to issue a series of directives to technology staff. The directives will include set account lockouts, enable audit processes, disable or rename guest accounts, and require all users to have passwords. As part of this effort, NMAI will establish a process to document server settings for hardware and software for servers at NMAI locations and circulate this to appropriate technology staff. These directives will be incorporated into Service Level Agreements with OCIO. Provisional actions will be set in place immediately.	June 1, 2003 ¹
		Access to administrator group privileges will be limited to network and system administrators, authorized contractors, and key ITR staff.	March 28, 2003
		NMAI users will be asked to read and sign statements acknowledging compliance with SI Directive 931, <i>Use of Computers and Networks</i> , August 5, 2002.	March 28, 2003

¹ NMAI is in the process of hiring a new Technology Manager who will assume on-going responsibility for these actions.

		<p>members' Individual Development Plans as part of the IT Work Plan and evaluate performance and results at the mid-year review.</p> <p>We will reconsider security training needs and set goals for training money as part of the establishment of work plans for FY 04 fiscal year.</p>	<p>August 2003</p> <p>October 2003</p>
<p>4. Develop and implement a semiannual assessment process for systems and network assets that includes server configuration evaluations and network scans based on industry standards.</p>	<p>Concur</p>	<p>This task will be incorporated into the performance review of the Technology Manager. The Technology Manager will request staff to apply the "Windows Security Scoring Tool" on a quarterly basis and report the results to the ITR Manager.</p> <p>The Technology Manager will monitor and report on a quarterly basis to the ITR Manager compliance by Systems Administrators to install service packs and hotfixes.</p>	<p>March 2003</p> <p>March 2003</p>
<p>5. Review and determine the necessity of the numerous user accounts.</p>	<p>Concur</p>	<p>As a matter of policy, all NMAI systems administrators will be requested by the ITR Manager</p> <ul style="list-style-type: none"> ▪ To investigate the feasibility of implementing application specific non-expiring passwords. Some applications such as GroupWise are beyond the control of NMAI. We will set regularly expiring (90 day) passwords to applications that support this capability. ▪ To provide all NMAI users with the password policy when setting up new users. ▪ To review all existing user accounts and delete accounts for which no user exists. 	<p>January 28, 2003</p>

6. Review the current system configurations and make adjustments where necessary to enhance system security.	Concur	The Technology Manager will provide a monthly report to the ITR Manager on the status of current systems configurations and plans for enhancing system security. Systems security maintenance will be incorporated into the Technology Manager's performance plan.	April 28, 2003 ²
--	--------	--	-----------------------------

B. Automated Information Systems Developments

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. Define an NMAI sponsor and formally define a development implementation team for the collection management system, media information management, and contact management system.	Concur	In regard to NMAI's Collections Information System (CIS): We established a staff team to develop requirements and select the CIS and we will name a development team, led by a newly established Collections Information System Manager, in February 2003. The CIS implementation team will include OCIO staff and a contract Unix systems administrator.	February 28, 2003
		In regard to the Media Information Management System, NMAI will establish an implementation team when the Media Technology Working submits its recommendations to the CIO for inclusion in the Technology Reference Manual. We plan to acquire a system in Third Quarter FY03.	June 6, 2003
		In regard to the Contact Management System, pending formal approval of NMAI's Senior Management Group, Joan Andrews will be appointed to lead the Contact Management implementation team.	February 28, 2003

² This will be one of the first actions requested of the new Technology Manager. In the meantime, the Information and Technology Resources manager will as lead technology staff at the CRC, GGHC, and L'Enfant Plaza to provide a report and update plans for system security enhancement.

2. Require that current and future development projects follow the SI Life Cycle Management Policy.	Concur	NMAI's ITR Manager has instructed staff to follow recently issued institutional guidance provided by <i>Technical Standard & Guideline IT-920-01 Life Cycle Management Manual</i> .	December 12, 2002
---	--------	---	-------------------

C. Disaster Recovery and Continuity of Operations Plan

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. We recommend that the Director, National Museum of the American Indian, adopt and implement a disaster recovery and continuity of operations plan in accordance with SI policies or current industry standards.	Concur	<p>We note that OCIO plans to issue <i>TSG IT-960-02, Disaster Recovery and Contingency Planning</i> in December 2002. The ITR Manager will review the Policy and discuss with staff how best to develop, adopt, and implement a Disaster Recovery and Contingency Plan.</p> <p>NMAI will appoint the new Technology Manager to oversee the development an NMAI Disaster Recovery and Contingency Plan.</p> <p>The ITR Manager will request the new Technology Manager to implement the plan either as directed by the Policy document or by July 2003.</p>	<p>January 4, 2003</p> <p>March 21, 2003</p> <p>July 25, 2003</p>

D. Segregation of Duties and Change Management Process

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
<p>1. Assign contract oversight responsibilities for technical contracts to qualified information technology staff.</p>	<p>Concur</p>	<p>Unfortunately NMAI has not had sufficient information and technology staff to dedicate to the support of its systems. In striving to open three buildings in ten years, NMAI dedicated a large part of its technology resources to desktop support staff. As part of a reassessment of its information and technology staff, NMAI understands and supports the urgent need to provide more technical support for computer applications managed independently by non-technical staff. NMAI requested two new FTEs in FY03 to strengthen this area. These two positions should be filled by June 2003.</p> <p>ITR staff will work closely with COTRs managing technical projects to provide contract oversight support for technical issues. ITR staff will apply Life Cycle Management guidelines to legacy systems.</p> <p>We note that FARSIGHT does not commit or expend funds. It is a "cuff record" financial tracking system that enables NMAI management to monitor and plan NMAI's budget and provides functions not available in SFS. All financial obligations take place within PeopleSoft, SI's ERP.</p>	<p>June 2003</p>

Define and implement, with support from the Office of Contracting, a contract modification for the maintenance of system support technology contracts.	Concur	NMAI will review the existing contract for the FARSIGHT vendor and, with support from the Office of Contracting, specify systems maintenance requirements.	April 2003
2. Obtain the system documentation, including changes, from the FARSIGHT contractor and establish a change and configuration management process for future modifications.	Concur	System documentation will be requested immediately and a change and configuration management process will be established by the end of March 2003.	December 24, 2002 March 28, 2003
3. Perform an information technology organization assessment to include considering realigning technology positions under a central manager.	Concur	NMAI began this task in November 2002. The ITR Manager will present a draft proposal to NMAI's senior management group by April 25, 2003. The proposal will be reviewed, revised, and presented to NMAI's Technology Committee of its Board of Trustees in June 2003.	April 25, 2003 draft proposal June 2003 Board of Trustees Review

E. Systems Facilities Physical Conditions

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. Relocate the copiers from the computer rooms and relocate the routers and servers from	Concur	Plans are already underway to relocate the copier from the Network Control Center at the CRC to a different location.	February 2003

publicly accessible spaces.		<p>At the Research Branch, Bronx, plans are underway to put the router into a locked cabinet in the demark location.</p> <p>NMAI's L'Enfant Plaza offices do not have a computer room to house the servers for Raiser's Edge and FARSIGHT. We will consider the feasibility of placing these servers in the CRC computer room, the OCIO computer room in A&I, or propose a non-public space at L'Enfant Plaza.</p>	<p>February 2003</p> <p>May 2003</p>
2. Examine staff access needs and storage requirements at the GGHC computer room and develop controls to prevent public access to the system resources.	Concur	<p>Discussions are underway with GGHC management to determine alternative office and storage areas for the Film and Video contractor now sharing computer room space. NMAI's Deputy Director has tasked the ITR Manager and GGHC management to produce a new space plan to address these concerns.</p> <p>The video-conferencing equipment, now stored in the GGHC computer room, will be moved to a new location.</p>	<p>May 2003</p> <p>March 2003</p>
3. Permit the GGHC computer facilities to be used only for maintaining computer resources.	Concur	As stated above, we will move staff around to accommodate this recommendation.	May 2003

4. Establish a separate lock and key at the Bronx location and identify appropriate staff to maintain the key.	Concur	GGHC Security has been requested to install a new lock cylinder at the Research Branch, Bronx and discussions have taken place to identify appropriate staff to maintain the key.	January 2003
5. Install hand held extinguishers in computer rooms.	Concur	Technology staff are researching appropriate hand-held fire extinguishers for NMAI's computer rooms. Fire extinguishers will be purchased in January.	January 2003
6. While awaiting SI policies on computer rooms, issue guidance to staff on the need to maintain a safe working environment and reinforce more oversight of the computer rooms.	Concur	The ITR Manager will speak with staff and issue written guidance.	January 2003
7. Implement a back-up and emergency power supply to secure NMAI system resources.	Concur	The CRC computer room is connected to the back-up generator and has UPS units in place. Myro Riznyk, GGHC Facilities Manager, is investigating whether the New York computer facilities can be tied into the back-up generators at the GGHC and Research Branch. Access to the back-up generator may be subject to GSA provisions for the Custom House Building. If access is not granted, NMAI will acquire 30 minute UPS.	June 2003

8. Complete the necessary additions to the GGHC computer room and assess the overhead plumbing situation.	Concur	Myro Riznyk, GGHC Facilities Manager, is investigating the feasibility of installing drain pans in the GGHC computer room. Once storage and staffing relocations decisions are made, the necessary additions to the GGHC computer room will be undertaken. The ITR Manager, as part of the emergency supplies, require plastic sheets to be available to drape over machines.	July 2003
9. Establish procedures and persons responsible for maintaining proper housekeeping.	Concur	The ITR Manager will establish procedures and task staff with responsibility for maintaining proper housekeeping.	January 2003

F. Isolated NT Network

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. We recommend that the Director, National Museum of the American Indian, eliminate the <i>Windows NT</i> network.	Concur	The ITR Manager will contact SI's technology support contractor, Infostructures, and request contract support to migrate the Registration Information Tracking (RITS) application to be accessible through the Novell network.	April 2003

G. Peer-to-Peer Technology

<u>Recommendation</u>	<u>Response</u>	<u>Action</u>	<u>Target Date</u>
1. We recommend that the Director, National Museum of the American Indian, perform periodic network and PC reviews to determine if p2p programs are being used and take appropriate administrative action when necessary.	Concur	The Information and Technology Resources manager will task staff to perform regular network and PC reviews to determine if p2p programs are being misused. The Manager will issue guidance to staff about the use of p2p software to download copyrighted materials and will take appropriate administrative actions.	March 2003



Smithsonian Institution

Memo

Office of the Chief Information Officer

Date January 9, 2003

To Thomas D. Blair
Inspector General

cc L. Small, R. West

From *Dennis Shaw*
Dennis Shaw
Chief Information Officer

Subject Response to the Inspector General's Draft Report on Audit of Information System
Controls at the National Museum of the American Indian

Thank you for the opportunity to comment on the draft audit report on the National Museum of the American Indian's information system controls. We agree with the audit findings and report recommendations directed at my office. Planned actions associated with each recommendation are contained in the attachment.

Please call me on 202-343-1052 or George Van Dyke on 202-357-4235 if you have any questions.

Attachment

Arts & Industries Building Room 2361
900 Jefferson Drive SW
Washington DC 20560-0463
202.343.1052 Telephone
202.312.2884 Fax

Attachment

Response to Audit Report Recommendations on NMAI's IS Controls

Recommendation 1: Issue policies and guidance on the use of p2p technology for the Institution.

Response: Concur. The OCIO will analyze options for implementing adequate safeguards for peer-to-peer technology including instant messaging. Once we have completed our analysis we will issue policies and guidance on the use of peer-to-peer technology by July 2003.

Recommendation 2: Modify the SI network control points to identify large file transfers and potential file sharing activities in order to alert network administrators.

Response: Concur. The OCIO will upgrade the software in SInet routers (network control points) by October 2003. The software upgrade will allow the routers to recognize network applications and restrict this application traffic.