AUDIT REPORT

SMITHSONIAN TROPICAL RESEARCH INSTITUTE
INFORMATION SYSTEMS REVIEW

Number A-03-04

March 27, 2003

SUMMARY

The Office of the Inspector General audited information system controls at the Smithsonian Tropical Research Institute (STRI). The purpose of the audit was to evaluate information system controls regarding system access, server and network security, change and configuration management, physical security, and disaster recovery.

The following points were considered throughout our audit. Adequate security of information resource systems is a fundamental management responsibility. Of necessity, management must strike a reasonable balance between information technology security and operational capability.

We conducted interviews regarding the daily administration of technology resources with staff from STRI Information and Technology. We also spoke with representatives from the HSBC Bank. Through interviews, we gained an understanding of the practices employed concerning system configuration, network analysis, system access, disaster recovery, change management, physical conditions, and financial wire transfers.

Overall, STRI did have some system security controls in place regarding system backup. However, we determined that STRI system security configurations and safeguards were inadequate and the risk to system access and data integrity was high. 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 11 recommendations to improve systems security and general system controls at STRI. The recommendations to STRI included:

- secure current identified vulnerabilities;
- perform a systems security review as defined in Smithsonian Technical Standard and Guideline IT-930-01, Automated Information System Security Planning;
- develop and implement a semiannual security assessment process for system and network assets based on Office of the Chief Information Officer and industry standards;
- use technical guidance to develop, document, update, and implement server and client configuration settings;
- develop and implement a disaster recovery plan in accordance with Smithsonian policies and industry guidance;
- develop and support network and server security training specific to STRI technology staff system administration responsibilities;
- perform periodic network and personal computer reviews to determine if peer-to-peer programs or any other unauthorized programs or services are installed;
- reinforce the necessity for all STRI system passwords to comply with Office of the Chief Information Officer password standards;
- disable, rename, or remove all unnecessary user accounts;
- remove the folders and files containing images supporting the external private website; and

- adjust all STRI websites to ensure that a privacy statement is included as well as ensure that the content is reviewed before the information is displayed on the website.

The Director of the Smithsonian Tropical Research Institute concurred with the audit recommendations and has already begun taking proactive measures to secure its system resources. Overall, we believe that the corrective actions taken are responsive to the recommendations.

Office of the Inspector General
Office of the Inspector General

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

FBI	Federal Bureau of Investigation
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
SANS	SysAdmin, Audit, Network, Security Institute
STRI	Smithsonian Tropical Research Institute
P2P	Peer-to-Peer
SD	Smithsonian Directive
SI	Smithsonian Institution

INTRODUCTION

A. Purpose

The purpose of the audit was to evaluate STRI information system controls for systems access, server and network security, system changes and configuration management, physical security, and disaster recovery planning.

B. Scope and Methodology

The audit was conducted from January 9, 2003, to February 27, 2003, in accordance with generally accepted government auditing standards. The audit methodology consisted of the following:

- identifying and reviewing applicable Institution policies and procedures related to system general controls, computer system security, and integrity of computer resources;
- comparing STRI's system security settings with industry and 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; and
- utilizing guidance issued by the National Institute of Standards and Technology, National Security Agency, and *Microsoft* Corporation relating to system security configuration, and disaster recovery planning.

We reviewed:

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

As part of our review, we conducted interviews with STRI technology and administrative staff, and support contractors. We spoke with staff from STRI Information and Technology and STRI contractors from HSBC Bank. Through interviews, we gained an understanding of the practices employed concerning system configuration, network analysis, system access, disaster recovery planning, and change management.

C. Background

The Smithsonian Tropical Research Institute has a 90-year history in Panama going as far back as construction of the Panama Canal. The Institute has a scientific interest in surveying the flora and fauna of the area for the purpose of controlling insect borne diseases such as yellow fever and malaria. STRI scientific staff is composed of 10 different nationalities and has a core staff of 33 scientists who are specialists in their field. In addition, STRI manages and administers its information technology resources locally.

RESULTS OF AUDIT

STRI Information System Security

Information system resources at STRI can be strengthened. Specifically,

- server configurations are not documented, not up-to-date, and do not meet industry standards;
- sensitive network and accounting system resources are vulnerable;
- no documented disaster recovery plan exists; and
- staff is using unauthorized peer-to-peer Internet file transferring programs.

STRI systems are at risk because its staff has not performed any recent system security assessments[1]. Without periodic system security assessments STRI system resources are vulnerable and not up-to-date and could compromise financial transactions and disrupt or cease network and computer operations.

Background

We evaluated STRI system security and disaster recovery plan at Panama City, Panama. We used Smithsonian Directives and industry guidance and standards from the National Institute of Standards and Technology, 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.[2]

Smithsonian Directive 115, *Management Controls*, revised July 23, 1996, lists standards that shall apply to Institution units. 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 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 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.

Smithsonian Institution Technical Standard & Guideline IT-930-01, Automated Information System Security Planning, Version 1.0, November 2002, provides guidance to IT managers in producing system security planning documents and describes security-related planning activities. It also explains how security requirements are generated,

[1] OCIO Guidance recommends performing security risk assessments to determine the extent of potential threats and risks with an automated information system throughout its life cycle. The output of this process helps identity appropriate controls for reducing or eliminating risks and vulnerabilities.
[2] Registry settings and *Novell* servers were not evaluated.

tracked, incorporated, and tested within the lifecycle. Implementation of a sound automated information system security planning process can help build a trusted environment and provide security necessary to conduct business electronically at and within the Institution.

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 manner. The TRM identifies Windows 2000 as the preferred desktop operating standard.

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.

Appendix A lists industry standards used to evaluate STRI information system resources.

Results

We evaluated STRI system configurations that included server and sub-network security. Under the current system configuration, we determined that STRI servers and network systems are vulnerable and should 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.[3] STRI falls in the low range of average scores with a score of 3.8. Table 1 summarizes the averages for hotfixes and server scores for each location. On a positive note, the servers were up-to-date on service packs.

Table 1. Averages Based on Center for Internet Security© Scores

	Average	ACCAPP Server	NAOSFTP Server	Webshield Server
No. of missing hotfixes and security patches	7.67	8	7	8
Missing service pack[4]	0	0	0	0
Score	3.8	3.8	3.8	3.8

[3] The Scoring Tool criteria are divided into four categories: (1) Service Packs and Hotfixes, (2) Policies, (3) Security Settings and (4) Available Services and Other System Requirements.
[4] STRI Windows NT servers had no missing service packs.

The failure to maintain servers with the most current versions is a risk that can be easily mitigated by maintaining software up-to-date with service packs and hotfixes.[5] 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.

Although a tape backup process is in place, STRI had not implemented a disaster recovery plan for IT services. A disaster recovery plan assesses the adequacy and ensures 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. Our evaluation of the physical server conditions identified a clean and secure environment. Server room access is restricted by a card reader lock, fire suppression is available, and access logs reviewed periodically.

As part of our network analysis, we performed network scans and limited penetration testing on the STRI network. Specifically, we researched and used the most common identified port and service vulnerabilities. We scanned the STRI network and were able to obtain access to critical computers and sensitive information at STRI. Table 2 shows a summary of weak computer access vulnerabilities and non-password compliance at STRI.

Table 2. Summary of STRI Network Analyses

Subnet	Computers Scanned	Passwords Compromised	Non Compliant Passwords	Blank Passwords	Administrative Accounts & Passwords Compromised	P2P Internet File Sharing Installed
232	32	39	55	16	41	16
233	105	26	26	12	16	1
234	86	11	11	10	7	0
235	2	0	0	0	0	0
236	12	0	0	0	0	0
237	11	1	1	1	0	0
238	52	13	13	7	12	0
239	97	20	20	13	16	3
Total	**397**	**110**	**126**	**59**	**92**	**20**
Percentage		**27.71%**	**31.74%**	**14.86%**	**23.17%**	**5.04%**

Our penetration testing successfully compromised STRI computers used by the accounting department to perform bank wire transfers and an IT department computer used to manage the STRI network resources. We were able to identify the accounting departments different wire transfers and timing pattern of its wire transfers. With this knowledge we could open any one and modify the electronic files that contained individual names, bank routing numbers, and amounts thereby possibly altering

[5] 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.

individual wire transfers that averaged about $21,000 every two weeks. Also, we were able to gain access to 110 STRI user accounts or 27 percent that included the main computer used to monitor and manage STRI network resources. A compromise of this machine could provide an opportunity to cause havoc to STRI and SI networks that includes disabling the STRI network communications.[6]

In addition, from our network scans and analyses, we identified a STRI computer that is being used to host files that link to a non-SI website. The website is of a former STRI employee. The former employee has since resigned and left STRI all together as of July 2001. Although STRI IT staff manages two web servers, we identified numerous other STRI computers accessible through the Internet and some were hosting web sites. For example, the NAOS Molecular Group maintains a website that links back to the STRI main page. However, the NAOS website does not contain a privacy statement and it contains a cartoon link that refreshes itself. The cartoons displayed on the NAOS website are questionable and could be viewed as inappropriate. In addition, there is no control on what type of images will be displayed since the cartoon is linked to a non-Smithsonian website. We also identified other computers with Apache web server operating systems that are vulnerable to several FBI and SANS Institute top 20 vulnerabilities.[7]

Further analyses of STRI computers identified that staff are using peer-to-peer programs such as Kazaa a well recognized Internet file transfer program. Use of peer-to-peer technology (p2p[8]) puts STRI systems and the SI network at risk. We found that staff was using p2p programs such as instant messaging and Internet file sharing programs. Instant messaging is used to communicate with others through the Internet and the file sharing program is used for personal downloading of music and video files. As a result, STRI and SI system resources are vulnerable to viruses, worms, and denial of service attacks.

Also, 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. Further, 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. Additional risks include copyright infringements and viruses and Trojan horse program propagation. STRI systems are at risk because the last system security assessment was performed in 1994. STRI IT staff relies on OCIO to provide guidance and assessments of its network, server, and desktop computers. Information technology staff has applied its security attention on keeping its Novell network and Novell file server's up-to-date and secure. In addition, according to STRI IT management, computer resources have not been upgraded to the OCIO Technical Reference Model because of budget funding limitations.

As a result, without periodic security assessments STRI system resources are vulnerable and could disrupt or cease network and computer operations. In addition, without

[6] Although access was gained to the wire transfer files, no files, accounts, or amounts were altered.
[7] The Apache web computers vulnerabilities include remote open secure socket layer vulnerable to the Slapper Worm virus, traversal encoding, and ping of death denial of service.
[8] 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.

standard security system configurations STRI system resources are vulnerable to unauthorized, undetected activities, and possible financial losses.

Conclusion

Based upon our configuration and network analyses, we believe that STRI can improve systems security by introducing an assessment process into its IT administration duties. Implementing security assessments and performing periodic network scans can identify risks thereby limiting vulnerabilities and preventing system compromises.

Recommendations

We made 11 recommendations to the Director, Smithsonian Tropical Research Institute:

1. Secure current identified vulnerabilities.

Management Comments

Concur. STRI IT staff has already begun updating its Windows NT servers and policies and security settings have been set in the Fundware server. Completion dates for the remaining Windows NT server is expected by April 25, 2003. Network scans have been performed and unauthorized ports and services will be closed by March 28, 2003.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

2. Perform a systems security review as defined in SI Technical Standard and Guideline IT-930-01, AIS Security Planning.

Management Comments

Concur. STRI IT staff plans to perform a systems security review according to SI Technical Standard and Guideline IT-930-01, AIS Security Planning with a planned completion date of June 27, 2003.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

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

Management Comments

Concur. Beginning in September 2003, a security assessment will be performed semiannually.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

4. Use technical guidance to develop, document, update, and implement server and client configuration settings that includes application servers, web servers, and any other computer that is accessible and used on the Internet.

Management Comments

Concur. Implementation of the Technical Reference Model was initiated in the beginning of 2003 and is contingent upon available budget. A target compliance date of August 29, 2003, is planned.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

5. Develop and implement a disaster recovery plan in accordance with SI policies and industry guidance.

Management Comments

Concur. Corrective action has been initiated based on SI and industry guidance and is contingent upon completion of recommendation two. September 26, 2003 is the planned target date.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

6. Develop and support network and server security training specific to STRI technology staff system administration responsibilities.

Management Comments

Concur. Management plans to provide Windows NT and 2000 security training to its server administrators and system security staff during the current fiscal year.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

7. Perform periodic network and PC reviews to determine if p2p programs or any other unauthorized programs or services are installed and take appropriate administrative action when necessary as well as removal of these programs and files.

Management Comments

Concur. Management has begun eliminating P2P and unauthorized programs. Planned completion date of July 25, 2003 is planned with future reviews performed semiannually.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

8. Reinforce the need that all STRI system passwords comply with OCIO password standards especially for information technology staff with administrative responsibilities.

Management Comments

Concur. Management plans that all passwords will comply with OCIO standards by July 25, 2003,

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

9. Disable, rename, or remove all unnecessary user accounts, particularly within the accounting department.

Management Comments

Concur. Management plans to remove all unnecessary accounts by July 25, 2003.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

10. Remove the folders and files containing images supporting the external private website.

Management Comments

Concur. The files supporting the external website have been removed as of February 27, 2003.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

11. Adjust all STRI websites to comply with SI standards of maintaining a privacy statement as well as ensuring content is reviewed before public display on the website.

Management Comments

Concur. Content of the website is being reviewed by the Office of Public Information with a target completion date of April 30, 2003.

Office of the Inspector General Response

The Director's actions are responsive to the recommendation.

Appendix A. Industry Standards

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

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.

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. This guidance defines the purpose of computer security as a way to protect an organization's valuable system resources, 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.

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.

SysAdmin, 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; and
- Internet protocol and machine name disclosure outside the internal trusted network and firewall circumvention.

Appendix B. Management Comments from Dr. Ira Rubinoff, Director, STRI

Smithsonian Tropical Research Institute Memo

Office of the Director

Date March 13, 2003

To Thomas D. Blair, SI Inspector General

cc SI: Dennis Shaw, Jason-Robert Scott, David Cole
STRI: Georgina de Alba, Francisco Rivera

From Ira Rubinoff

Subject Review of draft audit report on information system controls at STRI

Thank you for the opportunity to review the audit report on Information Systems Controls at STRI. We concur with all the recommendations of the report and in concurrence with the STRI IT department, the corrective action and target date for completing the action are indicated after each recommendation.

STRI has a total of twelve servers. Eight servers use Novell as the network operating system and four servers use Windows NT. The report concentrates in the Windows NT environment. Novell servers were not evaluated during the audit. Our Novell servers are up-to-date and secure.

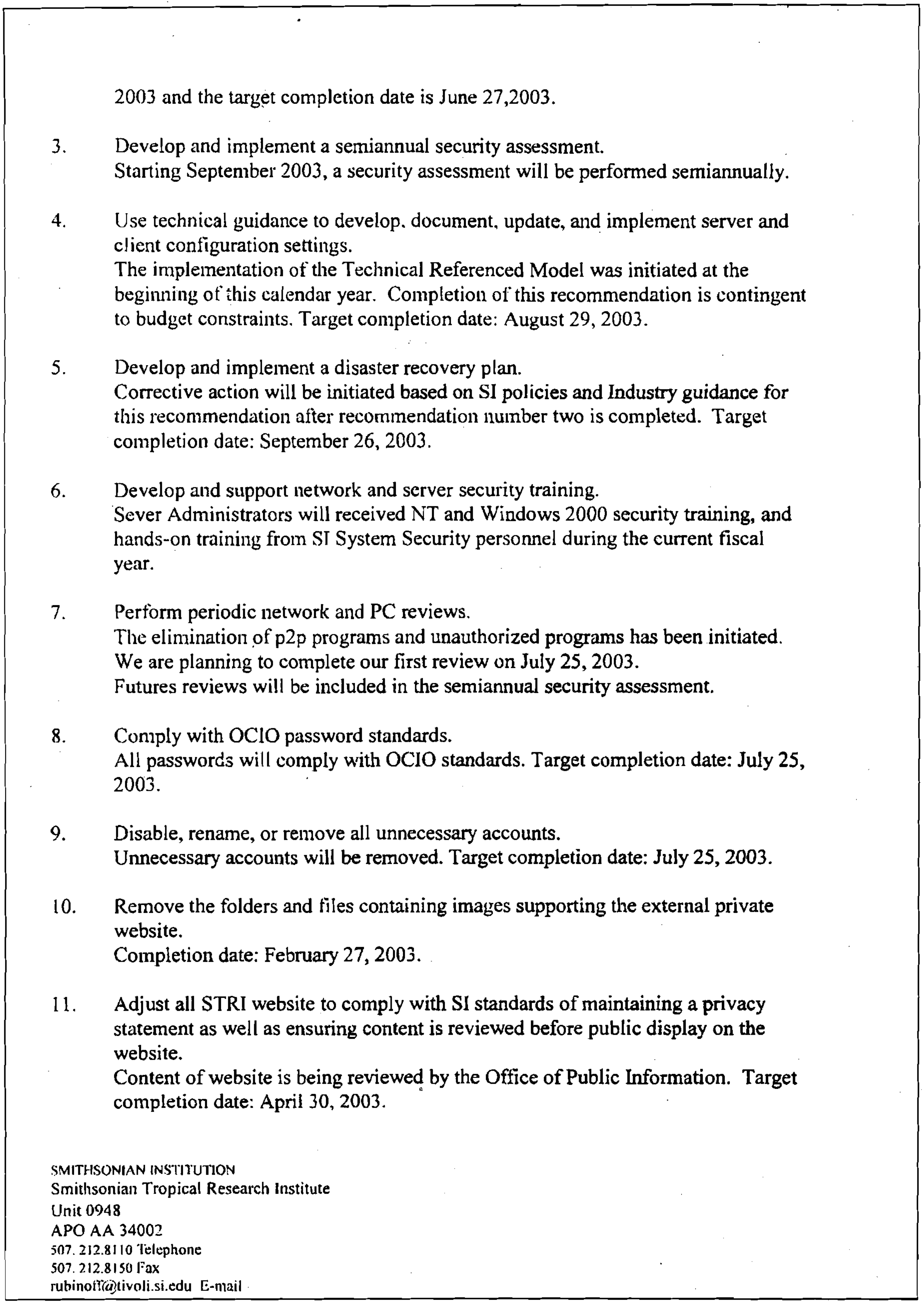
Recommendations and Corrective Actions.

1. Secure Current Vulnerabilities.
   a) Hotfixes and patches.
   We started to update all Hotfixes and Patches in our NT servers on February 17, 2003. Target completion date: April 25, 2003.

   b) Policies and Security Settings.
   Policies and Security Settings have not been set in the Fundware server. Polices and Security Settings were completed in the remaining NT servers on February 28,2003. Target completion date: March 28, 2203.

   c) Ports and Available Services.
   Scans were performed. As a result, ports and services that were not authorized to the users were closed as detected. Target completion date: May 30,2003.

2. Perform a Systems Security Review.
   A Systems Security review will be performed according to SI Technical Standard and Guideline IT-930-01, AIS Security Planning. The review will initiate in April



2003 and the target completion date is June 27,2003.

3. Develop and implement a semiannual security assessment.
Starting September 2003, a security assessment will be performed semiannually.

4. Use technical guidance to develop, document, update, and implement server and client configuration settings.
The implementation of the Technical Referenced Model was initiated at the beginning of this calendar year. Completion of this recommendation is contingent to budget constraints. Target completion date: August 29, 2003.

5. Develop and implement a disaster recovery plan.
Corrective action will be initiated based on SI policies and Industry guidance for this recommendation after recommendation number two is completed. Target completion date: September 26, 2003.

6. Develop and support network and server security training.
Sever Administrators will received NT and Windows 2000 security training, and hands-on training from SI System Security personnel during the current fiscal year.

7. Perform periodic network and PC reviews.
The elimination of p2p programs and unauthorized programs has been initiated. We are planning to complete our first review on July 25, 2003.
Futures reviews will be included in the semiannual security assessment.

8. Comply with OCIO password standards.
All passwords will comply with OCIO standards. Target completion date: July 25, 2003.

9. Disable, rename, or remove all unnecessary accounts.
Unnecessary accounts will be removed. Target completion date: July 25, 2003.

10. Remove the folders and files containing images supporting the external private website.
Completion date: February 27, 2003.

11. Adjust all STRI website to comply with SI standards of maintaining a privacy statement as well as ensuring content is reviewed before public display on the website.
Content of website is being reviewed by the Office of Public Information. Target completion date: April 30, 2003.