GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

# APPLICATION OF THE NSA INFOSEC ASSESSMENT METHODOLOGY

# FOR

# GIAC INTERNATIONAL SCHOOLS, INCORPORATED WASHINGTON, DC

## JANUARY 2000

PREPARED BY:

**KATHRYN CROSS**
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b

THE INFORMATION CONTAINED IN THIS REPORT WAS DERIVED FROM PROPRIETARY DATA PROVIDED BY GIAC INTERNATIONAL SCHOOLS, INCORPORATED

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## Table of Contents


I. ABSTRACT ..... 3

II. NSA INFOSEC ASSESSMENT METHODOLOGY.....3

III. SAMPLE NSA INFOSEC ASSESSMENT ..... 4

INTRODUCTION ..... 4

SYSTEM DESCRIPTION..... 5

INFOSEC ANALYSIS..... 7

INFOSEC Documentation.....7
INFOSEC Roles & Responsibilities.....8
Identification & Authentication.....9
Account Management.....10
Session Controls.....11
External Connectivity.....12
Telecommunications.....13
Auditing.....14
Virus Protection.....14
Contingency Planning.....15
Maintenance.....17
Configuration Management.....18
Back-Ups.....19
Labeling.....20
Media Sanitization/Disposal.....20
Physical Environment.....21
Personnel Security.....21
Training and Awareness.....22
Risk Assessment.....23

CONCLUSION….....24

References.....26

APPENDICES ..... .28

APPENDIX A –SYSTEM DIAGRAMS..... 28
APPENDIX B – DOCUMENTS REVIEWED..... 29
APPENDIX C – POSITIONS INTERVIEWED..... 30


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## I. ABSTRACT

Presidential Decision Directive 63 (PDD 63), signed by President Clinton on May 22, 1998, established the importance of protecting the United States' critical infrastructures, defined as, "…those physical and cyber-based systems essential to the minimum operations of the economy and government." PDD 63 declares that infrastructure protection is necessarily a shared responsibility between the civilian economy and government as both sectors would be likely targets of attacks. PDD 63 establishes a framework for a National Infrastructure Assurance Plan, including the requirement that "frequent assessments (…) be made of critical infrastructures' existing reliability, vulnerability, and threat environment", and that the National Security Agency (NSA) "provide assessments encompassing examinations of [the susceptibility of] U.S. Government systems to interception and exploitation" (Presidential Decision Directive/NSC-63).

NSA's INFOSEC Assessment Methodology (IAM) is a standardized baseline analysis for information security (INFOSEC) used to meet the assessment requirement levied by PDD 63. The IAM grew out of NSA's experience conducting information systems security inspections for its government customers over a span of fifteen years. The assessment is a systematic, comprehensive evaluation of a company or agency's information system strengths and vulnerabilities. The IAM includes detailed recommendations to eliminate or mitigate any security issues identified by the assessment. Because the market created for the IAM vulnerability assessments by PDD 63 is very large, NSA does not have the resources to perform all of the requested assessments. Accordingly, NSA has responded by developing the two-part INFOSEC Assessment Training and Rating Program (IATRP). The first part of the IATRP is a course designed to train INFOSEC professionals in the IAM; the second part is an appraisal of INFOSEC Assessment Capability Maturity Model (IA-CMM) which NSA conducts for service providers who wish to be rated on their ability to conduct NSA IAM assessments (Digital Knowledge).

This paper will look at the structure of the NSA INFOSEC Assessment Methodology and provide an example of the use of the IAM for a fictitious firm, GIAC International Schools, Inc.

## II. NSA INFOSEC Assessment Methodology (IAM)

The NSA INFOSEC Assessment is conducted by a team of individuals who review the information system security posture of a specified, operational system for the purpose of identifying potential vulnerabilities and recommending steps for eliminating or mitigating those vulnerabilities. The assessment typically consists of a pre-assessment phase, an on-site visit, and a post-assessment phase, the end result of which is a detailed report of findings and recommendations. The INFOSEC assessment addresses each of eighteen different areas specified in the IAM: INFOSEC Documentation, INFOSEC Roles & Responsibilities, Identification & Authentication, Account Management, Session

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Controls, External Connectivity, Telecommunications, Auditing, Virus Protection, Contingency Planning, Maintenance, Configuration Management, Back-ups, Labeling, Media Sanitization/Disposal, Physical Environment, Personnel Security, and Training & Awareness (National Security Agency, a).

In the pre-assessment phase the IAM team refines the customer's needs, gains an understanding of the criticality of the customer's information, identifies the system to be assessed, coordinates logistics with the customer, and devises an assessment plan. This phase begins with a one to two day visit to the customer's site to meet with key points of contact, develop an understanding of the organization's mission, and meet with system owners. From this visit the assessment team determines information criticality, systems criticality, and any special considerations, concerns or constraints levied by the customer organization. The team establishes the scope of the assessment and requests necessary system documentation from the customer. After the initial visit, there is a two to four week period in which the assessment team reviews documentation, conducts a preliminary analysis of the system, establishes the activities to be conducted during the on-site activities phase of the assessment, and formalizes the written Assessment Plan Outline which documentss: Important Points of Contact, Organizational Mission, Organizational Information Criticality, System(s) Information Criticality, Customer Concerns, System Configuration, Individuals and Positions to be Interviewed, Documents Reviewed, and the Timeline of Events (National Security Agency, b)

The purpose of the on-site activities phase is to explore and confirm the information received during the pre-assessment phase; to perform data gathering and validation through interviews with key personnel, review of systems documentation, and systems demonstrations; and to provide initial analysis and feedback to the customer. This phase typically lasts one to two weeks.

During the post-assessment phase the team conducts an additional review of the documentation, performs further analysis based on information gathered during the on-site visit, finalizes its analysis, prepares the final report and presents its findings to the customer. The duration of the post-assessment phase can vary from two to six weeks.

## III. Sample NSA INFOSEC Assessment

### Introduction

This INFOSEC assessment was performed at the headquarters of GIAC International Schools, Incorporated located in Washington, DC. A subsidiary of Global Information Assurance Corporation, GIAC International Schools, Inc. (GISI) is a worldwide firm providing education to students who are dependents of American citizens and other foreign nationals in locations around the world. Over 100,000 students are enrolled in GISI schools and are served by some 7,000 educational staff and 400 support staff located in the three area and twenty district offices in the United States, Europe, and the Pacific as well as in the schools themselves. GISI is headed by a director who oversees

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

all agency functions from GISI headquarters located in Washington, DC. Each of the GISI areas is managed by an area director. There are two additional directors, the GISI Associate Director for Education and the Associate Director for Management, whose offices and staffs are located at the headquarters. Approximately 400 employees work at the Washington headquarters which houses the management divisions of Personnel, Procurement, Logistics, and Information Technology as well as the Office of the Comptroller and the Office of Communications.

This INFOSEC assessment was performed during January 2003 on the headquarters' computer network operated by the GISI Information Technology Division Operations Branch. The assessment methodology was modeled on the National Security Agency's Information Systems Security Assessment program and consisted of a Pre-Assessment phase, an On-site Visit, and a Post-Assessment phase. Headquarters Operations Branch personnel provided information concerning systems, connectivity, and policies and protection measures currently in place. In the pre-assessment phase, the assessment team conducted interviews with the headquarters business units, the Chief Information Officer (CIO), the Chief Technology Officer (CTO), and key members of the Director's staff and the staffs of Associate Directors for Education and Management as well as with key members of the IT Operations Branch staff and the Information Security System Manager (ISSM). During the on-site visit, further interviews were conducted including interviews with users and with contractor computer maintenance and help desk personnel. Systems demonstrations and tests provided additional information regarding the effectiveness of existing protective measures. In addition, the assessment team consulted the results of an information security penetration test recently conducted by a consulting firm on behalf of the ISSM.

This INFOSEC assessment is not an inspection, certification, or risk analysis. Implementation of the recommendations contained in this document is at the discretion of GISI management and is strictly voluntary. The implementation of any or all recommendations contained herein does not guarantee the elimination of all risks.

## System Description

The mission of GISI Headquarters is to provide support and direction to the GISI schools in Europe, the Pacific, and the United States. The highest level of data processed by headquarters file and database servers is sensitive but unclassified (SBU). Much of this data is stored only at the headquarters location. Although the current Continuity of Operations Plan does not refer to the importance of IT disaster recovery, interviews with key management personnel indicate that the agency would need to recover its IT operations within two weeks of the cessation of normal operations. GISI's Organizational Information Criticality matrices (National Security Agency, b, pp. 10-12) are displayed below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

| Criticality Definitions | Confidentiality (C) Integrity (I) Availability (A) |
|---|---|
| High | • (C) Information is sensitive but unclassified; inappropriate release would violate the FERPA or potentially endanger lives.<br>• (I) Unauthorized of unintentional modification could result in fraud, legal issues, or serious embarrassment to the agency.<br>• (A) Unavailability could result in inability to meet payroll obligations or to meet critical mission requirements. Information must be available within 24 hours. |
| Medium | • (C) Information is considered confidential; its disclosure could prove embarrassing to the agency.<br>• (I) Loss of data or unauthorized changes to data will require significant investment to recover; but data is available for re-entry.<br>• (A) Information availability is of moderate concern. Recovery must be accomplished within 10 days. |
| Low | • (C) Information is for public consumption and/or its compromise would in no way be harmful to GISI operations.<br>• (I) Changes to data would be inconvenient, but could be easily recognized and rectified.<br>• (A) Data is readily available elsewhere and/or data recovery within 30 days is satisfactory. |

| ORGANIZATIONAL INFORMATION CRITICALITY | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Electronic Mail | H | M | M |
| Student Information | H | M | L |
| Employee Information | H | M | M |
| School Information | H | M | L |
| Distance Education Content | L | M | M |
| Public Web Server Content | L | M | M |
| File Server Content | H | M | M |
| **Aggregate** | **H** | **M** | **M** |

| ORGANIZATIONAL SYSTEMS CRITICALITY | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Electronic Mail System | H | M | M |
| HQ Database Servers | H | M | L |
| HQ File Servers | H | M | M |
| Web Servers | H | M | M |
| Distance Education Servers | H | M | L |
| **Aggregate** | **H** | **M** | **M** |

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The GISI headquarters' local computing environment (LCE) includes approximately 450 desktop computers running Microsoft Windows NT 4.0 or Windows 2000. A limited number of workstations run Microsoft Windows 98 (10) or a Macintosh OS (12). In addition, telecommuters and employees who are TDY use approximately 70 laptop computers running either Windows NT or Windows 2000. The headquarters has approximately 400 employee user accounts.

Outward facing servers, including DNS servers, Lotus Notes servers for Distance Education programs, and the Netscape iPlanet or Windows IIS web servers with non-secure content, are housed in a DMZ. Windows Domain Controllers, Microsoft Exchange mail servers, Oracle (Unix OS) database servers, secure content web servers and Novell file servers sit in a separate internal zone. The LCE is protected behind a high availability (HA), clustered Check Point firewall configured on Nokia appliances; the Cisco routers that connect the LCE to the Internet also provide a measure of protection via access control lists. The DMZ is a "poor man's DMZ", configured off the single set of firewalls. The firewall is also the terminus for the GISI Virtual Private Network (GVPN), built on Check Point's VPN-1/Firewall-1 and VPN-1 Secure Client software.

Protocols in use include TCP/IP, IPX, HTTP, SMTP, FTP, SSL, SSH, and SNMP (internal network only). GISI's web servers housing secure applications have PKI certificates and access to secure applications is encrypted.

Connection to the Internet is via a partial T-3 line direct to UUNet (with a backup T-1 line that is used in the IT Test Lab until needed for production). Headquarters has a bank of 25 phone lines connected to a Shiva modem. Access to the Shiva requires a user account and password, but is available 24 x 7. As part of security modifications now underway, this modem bank is being replaced by the GISI VPN.

GISI has an Intrusion Detection System (IDS) in place which is operated and monitored by the Information Assurance office, under the direction of the ISSM.

Following Oar and Jackson's recommendations presented at the 21st National Information Systems Security Conference, GISI has adopted many of the standard information security procedures used by the Department of Defense including the approaches and disciplines defined by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (Oar and Jackson, 1998). In addition, the CIO and ISSM have incorporated a number of practices found in the Nation Institute of Standards and Technology (NIST) Special Publications 800 series which establish appropriate INFOSEC practices for the federal government.

## INFOSEC Analysis

### (1) INFOSEC Documentation

#### A. Finding:

There are a number of key INFOSEC policy documents that have not yet been signed by the Director, GISI. The current lack of a Configuration Management policy inhibits the GISI IT Operations staff from ensuring that desktop configurations remain standard and that users do not modify configurations or install unauthorized software on

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

their desktops. Similarly, there is no System Users' Security Manual because the Director has not yet signed off on the revised Computer and Internet Access Agreement which contains the Rules of Behavior for users. The lack of established policy in these and other areas leaves GISI computers and networks vulnerable to configuration and system damage from malicious software downloaded and installed by users, either intentionally or inadvertently.

IT Operations Branch Standard Operating Procedures (SOPs) range from exceptionally thorough to virtually non-existent. Lack of SOPs for some technical areas could mean loss of service when/if the incumbent leaves the undocumented position.

**B. Discussion:**

GISI security documentation is contained in GISI policy statements and memoranda, in the GISI Information Assurance Program Manual (IAPM) and in IT Operations Branch Standard Operating Procedure (SOP) documents. Overall, GISI has done a good job of documenting its information security posture. See Appendix B for a full list of documents consulted in this assessment.

The GISI IAPM contains the essentials of the agency's INFOSEC documentation. It is a comprehensive document, providing statements of GISI Information Assurance (IA) Policy, Minimum Security Requirements, Certification and Accreditation, Functional Roles and Responsibilities, Reporting Procedures and Incident Response, Security Training and Awareness Program, PKI and VPN Technologies, and Classified Processing Requirements. The IAPM document implements within GISI headquarters all overarching INFOSEC requirements.

Other information security related documentation is present in several of the Operations Branch Standard Operating Procedures (see Appendix B). A number of these documents are quite thorough (Electronic Mail Administration, Unix Server Administration); others are sketchy or non-existent (routers and firewalls, Novell server administration).

**C. Recommendation:**

1. Ensure that the Director, GISI realizes the significance of the documents that have been prepared for his signature and understands the negative impact of continuing to do business without configuration management and other important Information Assurance policies.
2. Require that all members of the IT Operations staff update their SOPs, and require that they achieve the level of completeness found in those SOPs that are exemplary.

**(2) INFOSEC Roles and Responsibilities**

**A. Finding:**

The Director, GISI, has appointed a Chief Information Officer (CIO) who is the Approving Authority for all INFOSEC related matters at GISI headquarters. The CIO also serves as the Certification Authority and he has appointed an Information Systems Security Manager (ISSM) who, in turn, has appointed an Information Systems Security Officer (ISSO).

**B. Discussion:**

The IAPM clearly delineates the INFOSEC roles and responsibilities within GISI. These are divided into four general categories: 1) GISI Management, 2) Information

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Systems Security Management, 3) Systems Administration, and 4) System Users. For each category of user the document clearly and thoroughly spells out their responsibilities with respect to policies, systems operations, incident prevention and response, and security training. (IAPM, pp. 26-31).

Review of system administrator (SA) and network administrators (NA) SOPs, however, indicates that the roles and responsibilities delineated in the IAPM have not yet been incorporated into the SOPs. Interviews with NAs and SAs and with systems users reveal that many are not aware of their responsibilities as outlined in the IAPM.

**C. Recommendation:**

1. The ISSM/ISSO should take action to ensure that all affected parties are aware of their INFOSEC responsibilities.
2. The Operations Branch chief should ensure that SA/NA responsibilities are acknowledged and reflected in their SOPs. (See "INFOSEC Documentation" section of this report.)
3. The ISSM/ISSO should incorporate an explanation of user responsibilities into the awareness and training program. (See "Training and Awareness" section of this report).

**(3) Identification & Authentication**

**A. Finding:**

The GISI IAPM specifies the essence of identification (user ID) and authentication (User ID and password) and assigns ultimate responsibility for both to the ISSO (p. 13). At this time GISI uses single-factor authentication for each login (user ID and password) required by the user. However, GISI employees have recently been issued Common Access Cards (CAC) and GISI expects to implement card readers on workstations and laptops within the next six to twelve months.

Neither the IAPM nor the individual System Administrators' SOPs address the need for strong administrative passwords or the frequency with which these should be changed.

**B. Discussion:**

Password policies established in the IAPM are reasonably strong and include:

- minimum of 8 characters
- combination of upper, lower, numeric and special characters
- change every 90 days
- non-disclosure to others
- inability to reuse recently expired password
- automatic account lockout after three unsuccessful login attempts.

In practice, however, this policy is only as strong as the settings on the systems that control user authentication (e.g., Novell authentication servers and Windows Domain controllers). These strong password policy settings are not specified in the system administrator SOPs, and to date only the minimum length, lockout, 90 day change, and non-reuse features are enforced by the system. Other than the semi-annual Penetration Test conducted by IA, no attempt is made to ensure that users are conforming to the IAPM policy. Indeed, because of the lack of a strong INFOSEC Training and Awareness program (see "Training and Awareness" section of this report), it is doubtful that users

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

know of the policy contained in the IAPM. Interviews with users indicate that users frequently share their passwords with their co-workers and with their supervisors.

As Drew Robb points out, “These days hackers don’t need to guess dates or pets’ names to crack a password. They use software tools that rapidly run through all possible combinations until they find the one that works” (p. 93). It is important that GISI strengthen their password control through enforcing the use of strong passwords and sufficiently frequent password change.

Moreover, Gartner and others point out that, “An authentication service using *only* one authentication factor may be vulnerable. Combining two or more factors provides greater security: Gartner defines this as **strong authentication**” (Allan, 2002).

When implemented, the use of CAC cards will strengthen the GISI Identification & Authentication posture by requiring two factor authentication (“something you know” and “something you have”) which is preferable to the current single-factor authentication (Kleckner, 2002). Moreover, GISI’s ultimate goal is for the CAC to replace existing proximity badges; when this feature is in place, it will be necessary for the user leaving a workstation to go to the restroom or to another location in the building to remove his/her CAC from the card reader attached to his workstation, effectively securing the workstation whenever the user is away. (Phillips, 2002)

**C. Recommendation:**

1. Include the Identification and Authentication requirements for users, as expressed in the IAPM, in each system administrator’s SOP. To the extent possible, enforce these requirements via system settings.
2. Require that the ISSO and or the SAs use commonly available password-cracking software on a monthly basis to ensure that GISI users’ passwords are not easily guessed. When an easily guessed password is discovered, require that user to change his/her password to one that is stronger. Periodically run the password cracking routine against the Windows SAM to determine the amount of time required to crack administrative passwords. Ensure that all administrator passwords are changed frequently enough to protect against this type of cracking.
3. Include education on the importance of password control in the INFOSEC awareness campaign and INFOSEC user training. (See “Training and Awareness” section of this report.)
4. Move to institute two-factor authentication as soon as possible.

**(4) Account Management**

**A. Finding:**

The GISI IAPM refers briefly to proper procedures and configuration for user, guest, default and administrator accounts on workstations and servers (p. 17). The electronic mail administrator’s SOP clearly addresses creating and deleting domain user accounts, however, there is no corresponding SOP for the Novell system administrator. This lack of consistent, documented procedures could result in weak control of user accounts, possibly leading to a breach of security.

Departed users’ accounts are not always disabled promptly, leaving the system open to possible compromise by a disgruntled user or someone who may know the departed user’s ID and password.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**B. Discussion:**

Interviews with GISI HQ system administrators indicate that proper precautions are taken when setting up GISI servers and workstations to ensure that unnecessary accounts are disabled and that default administrator accounts are renamed. Accounts are well managed; user accounts are deleted or disabled when users leave the organization, when passwords are compromised, or when user accounts are not user for a protracted period of time. Administrators and Help Desk personnel report, however, that they are not always informed when a user has left GISI; therefore accounts often remain active for up to several weeks after the user's last day of official duty.

User accounts are created only at the written request of the user's supervisor. The principle of "least privilege" is applied and access to IT resources and data is restricted "to the smallest population consistent with other business needs, based on the criteria [sic] of a clearly delineated 'need-to-know'." (The International Information Security Foundation, 1999). Users are required to sign a Computer Use and Internet Access agreement before their new accounts are created. However, the agreement that they sign has not been revised in the last five years; the revised version together with the recently developed "Rules of Behavior for GISI Computer Users" is waiting for the Director's signature. Also, users are not required to complete initial security training prior to being granted access to their accounts.

As Corbitt points out, "... user account management is essential for ensuring computer security. Without it many other security measures (for example, identification and authentication) are rendered ineffective" (p. 21). Accordingly, it is altogether fitting for GISI to invest significant time and manpower resources to ensure that account policies are clearly established and reviewed often.

**C. Recommendation:**

1. Ensure that account policies, as stipulated in the IAPM, are uniformly applied and documented in SOPs pertinent to all venues where accounts are created, including Shiva accounts for as long as that system remains in place.
2. Obtain a weekly printout from the Personnel Division listing users who have departed GISI during that week. Promptly communicate their departure to all system administrators to ensure that their accounts are disabled/deleted.
3. Encourage the Director, GISI to promulgate the new Computer Use and Internet Access agreement as soon as possible and to require that all new users complete their initial security awareness and training before being granted access to GISI systems.

**(5) Session Controls**

**A. Finding:**

GISI users must logon (with user ID and password) to their workstations and the network before being granted access to GISI electronic resources. Users receive a warning banner prior to logging on. Accounts are set to lockout after three unsuccessful logon attempts and administrator intervention is required to unlock the account.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

There is no account history banner displayed upon login, so there is no way for a user to know if his/her account has been compromised and someone else has logged in after they last logged out.

There are no preset system time outs; GISI users' access to the network is only forcibly terminated once each day (at 0100); otherwise they are free to remain logged in around the clock, whether they are working or not. It is not altogether uncommon for a user to be away from his or her workstation (or even gone for the day) and the user is still logged into the workstation and the network. This leaves the user's workstation and the GISI network resources vulnerable to someone other than the authorized user making use of the user's account.

Privileged account use is limited to the minimum number of users needing such access.

**B. Discussion:**

The GISI warning banner viewed by users prior to logging on and gaining access to GISI computer resources clearly states that they are using corporate computer equipment, that the equipment must be used for official GISI business only, that their activity is subject to monitoring, and that by choosing to log on to the GISI computer network they are agreeing to the foregoing conditions. The banner is currently displayed on all Windows workstations; GISI is in the process of enabling the display of a similar banner on the Macintosh machines

In general it is in GISI's best interest to tighten session controls insofar as it can do so without unduly restricting legitimate user access.

**C. Recommendation:**

1. After obtaining management support, IA should make all users aware of the potential security ramifications of leaving their workstations logged in while unattended. Users should be encouraged to lock their workstations whenever they are away from them and to logout completely at the end of their duty day. Following the awareness campaign, Operations Branch personnel should ensure that all user workstations are configured to engage the lock-screen when there is no activity for some (reasonable) preset period of time.
2. Systems and network administrators should work with the ISSO to develop other logout mechanisms/settings as may be helpful to the security of the network. Protective measures should be considered for all accounts, including especially those accounts with administrative access.
3. Particular attention should be paid to session controls as they pertain to the use of the GISI VPN which is currently in a testing phase.

**(6) External Connectivity**

**A. Finding:**

GISI headquarters is reasonably well protected from outside attack. Unneeded ports and services are disabled on the routers and firewalls that connect GISI to the Internet. Connectivity to the Internet is further protected by a HA firewall which is set to fail closed. Firewall and router activity is logged.

However, the current configuration of GISI's dial-in capability terminates inside the firewall. (See System Diagrams in Appendix A.) Although this access requires a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

user ID and password, if a particular user's account is compromised, traffic from the attacker would enter the GISI network without passing through the firewall.

**B. Discussion:**

GISI is connected to the Internet through twin firewalls, configured for fail over, provide simple packet filtering as well as more complex programming that directs Internet traffic to specific ports and/or specific servers. For example, all port 80 traffic is directed to the Web servers located in the DMZ, no other HTTP traffic is allowed into the enclave unless it has been requested by a user; all port 25 traffic is passed to the Exchange server, etc.

The lack of SOPs for firewall and router administration makes it difficult to know how much attention is paid to the firewall and router audit logs on a regular basis. They are maintained and are referred to whenever events dictate referring to the logs as an appropriate action, but it is likely that the logs can be used more proactively in the future.

Dial-up access is restricted to those employees who need to have remote access from home or while on travel. This access is controlled by user ID and password. As currently configured, this access poses a significant threat to the GISI network. The GISI VPN, now in a testing phase, is being activated in part to overcome this vulnerability.

**C. Recommendation:**

1. Continue with all due haste to bring the VPN into full production and eliminate the current dial-in arrangement and its associated vulnerabilities.
2. Prepare SOPs for router and firewall administration that include specific requirements for monitoring the audit logs. (See "Auditing" section of this report).

**(7) Telecommunications**

**A. Finding:**

Connection to the Internet is via partial T-3 to UUNet. GISI maintains a T-1 as a backup line.

GISI does not process classified information. Sensitive information passing from outside to inside the GISI enclave is handled via secure Web servers that establish SSL communication with the outside user.

The GISI VPN has been well designed and, when implemented, will provide secure, encrypted tunneling for remote users.

GISI electronic mail servers are well protected against Internet viruses and other forms of attack. GISI's electronic mail communication, however, is not protected by encryption and there is no assurance that some FERPA information is not passing through the GISI email system, potentially being subjected to eavesdropping and other forms of compromise (United States Department of Education).

**B. Discussion:**

GISI should shore up its protection of electronic mail message contents. As Avolio and Piscitello note, "Most corporate end users are blissfully unaware of the security risks inherent in plaintext email, which are susceptible to four types of attacks: eavesdropping, forgery, denial of origination and replay" (p. 2). Administrators should endeavor to ensure that email contents are secure on every router, server, and system

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the email traverses during transmission. In addition to protecting the message content from eavesdroppers (via some form of encryption), among the basics to be considered are confidentiality: a guarantee to the sender that only the intended recipient(s) can read the message; integrity: a guarantee to the recipient that the message hasn't been altered in any way during transmission; authentication: a guarantee to the recipient that the purported sender of the message is the actual sender; and non-repudiation: the other side of the 'authentication' coin, guaranteeing that the sender cannot plausibly deny that he created or sent the message to the recipient. (Aviolo & Piscitello, 2001)

**C. Recommendation:**

1. Apply a PKI certificate to the email server.
2. Study the use of digital signatures for GISI email as well as other means of providing confidentiality, integrity, authentication and non-repudiation.

**(8) Auditing**

**A. Finding:**

The GISI IAPM specifies the need for logging and auditing. The Director, GISI has issued an Administrative Instruction implementing the auditing policy and levying the requirement that GISI SAs collect and retain audit data. The policy specifies what is to be audited, and declares the responsibility for the SAs to "develop a formalized plan detailing the process by which they will create, maintain, and store comprehensive audit trails" (p. 15).

Examination of the SA SOPs gives no indication that they have fully complied with the terms of this policy. Failure to properly implement logging can result in either or both of (1) GISI being unable to determine and/or prosecute the perpetrator of malicious damage to GISI systems or data, or (2) failure to receive advance warning of impending damage to GISI systems or data by an attacker from either inside or outside the system.

**B. Discussion:**

As Corbitt observes, "... audit trails are an important facet of security. [They] can be used to reconstruct events leading up to a breach of security policy. Alternatively they can be used as a support for regular systems operations." Auditing is an area in which there is room for significant improvement at GISI. Audit logs are enabled on the routers and firewalls and, to some extent, on the various Unix, Novell, and Windows servers, but there is no uniform or comprehensive practice regarding the monitoring and use of those logs.

**C. Recommendation:**

1. Initiate a review of all Operations Branch SOPs with respect to auditing. Ensure that GISI SAs are familiar with the existing policy as signed by the Director.
2. Develop auditing SOP for each critical SA/NA; ensure that this SOP includes what is to be audited, where, how, and how long audit data is to be stored, as well as what, if any, events should trigger alerts to the SA and/or members of the IA staff.
3. Modify the IAPM to require that the ISSO conduct regular reviews of audit data.

**(9) Virus Protection**

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**A. Finding:**

GISI requires that all systems have antivirus software installed. New virus definition files are downloaded daily from the provider's site and posted to an internal server. Workstations are set to update automatically once each week. Updates can also be pushed by SAs to the local workstations whenever the new definitions become available. Antivirus files are installed on GISI servers by their respective SAs and are updated daily.

The IAPM does not define a clear sequence of actions to be taken in the event of a virus or other malicious attack. This could result in time being lost and the damage to GISI and other systems being more extensive than necessary.

All software is obtained from reputable sources and is tested in the laboratory before being installed on production equipment. Only the IT Division and/or its contractors can install software on systems connected to the network.

**B. Discussion:**

GISI has a strong antivirus program, protecting all systems against malicious applications such as viruses, Trojan horses and worms which can cause loss of function and/or data if computers become infected. Given the preponderance of such attacks that have been conducted via email over the last few years, the GISI Exchange team has chosen to block many of the kinds of attachments that are typically used as "carriers". This has drastically reduced the number of incidents that GISI HQ has to deal with. Moreover, GISI has taken steps to ensure that each user's workstation is configured to automatically check for antivirus definition updates on a regular basis and GISI has initiated a mechanism to allow immediate "pushing" of updated virus definition files whenever that becomes necessary.

While the possibility exists that viruses and other malware might be inadvertently downloaded from Internet sites, GISI has taken additional steps to protect its users by removing their accounts from the local administrators group on their workstations.

The combination of these two measures has drastically reduced the incidence of virus attacks over the last twelve months.

**C. Recommendation:**

1. GISI's antivirus posture could be improved by setting the workstations to update automatically each time the user logs in. Although there is some concern that this might place an undue burden on the network at peak times of the day, it is an area that should be investigated.
2. IA should develop a clear plan for dealing with virus and other malicious attacks. This procedure should be developed in conjunction with SAs and NAs as well as with Help Desk personnel. Once a procedure has been agreed to, it should be communicated to all GISI users and should become part of the regular Training and Awareness program.

**(10) Contingency Planning**

**A. Finding:**

The IAPM states that "a contingency plan must be developed for every essential GISI IT system". This requirement is implemented by the IT staff through its backup policy, its maintenance agreements with hardware and software vendors (usually

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

requiring a four-hour response time), and through the regular monitoring of the health of both hardware and software.

Servers and other key pieces of network equipment are connected to uninterruptible power supplies (UPS) and, wherever possible, redundant power supplies are connected to different UPS.

However, there is no plan in place for dealing with a site disaster. In the event of such a disaster, GISI headquarters would be unable to reconstitute its IT operations in any kind of timely fashion. Eventually this would have a deleterious effect on the accomplishment of GISI's mission.

**B. Discussion:**

GISI IT conducts weekly full and daily differential backups of all of its servers and their data. IT staff is in the process of fully documenting the configuration of all of its servers and other key pieces of equipment. Provision should be made, however, for storing all of this information in a secure offsite location so that it would be available in the event of a site disaster.

One of the Generally Accepted System Security Principles is that "Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations" (The International Information Security Foundation, p. 46). The GISI Continuity of Operations Plan (COOP) signed by the Director declares that "GISI headquarters operations are deemed non-essential to the continued operation of schools during a national or natural emergency or crisis." The memorandum further specifies that, in the event of a "catastrophic disruption of GISI headquarters operations ... key management personnel [would] direct recovery operations from an alternate work site. Although the document specifies locations to which "key management staff" would relocate, and states that "to the extent practical, key management staff will telecommute from residences as temporary or permanent work sites are identified", the document makes no reference to any attempt to reconstitute IT operations.

**C. Recommendation:**

1. IT staff should discuss with upper management the importance of reconstituting IT operations in the event of a site disaster. Assuming this is seen to be a need, GISI management should conduct a study to determine mission or business critical functions and the period of time that GISI can survive without them.
2. With output from the study above, the IT Division should then build a contingency plan addressing the recovery of those functions within the time span allowed. The plan should include specific responsibilities and personnel who will accomplish them; including backup personnel if primary named personnel are unavailable. The plan should also have clear timelines and methods for accomplishing its objectives. If necessary, the plan should identify and prepare an offsite facility to restore those IT functions deemed critical. This plan should be presented to management and, after agreement is obtained, the plan should be periodically tested. The completed plan should be stored offsite as well as onsite in locations clearly specified and available to all key personnel.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**(11) Maintenance**

**A. Finding:**

The GISI IAPM specifies that the SA/NA is responsible for maintaining the system in a manner consistent with the System Security Accreditation Agreement (SSAA). Interviews with SAs, however, indicate that they are not aware of the existence of (or the content of) an SSAA for their systems. This lack of communication may mean that key systems are not being maintained in accordance with INFOSEC policy.

All GISI SA/NA personnel are American citizens and have had background checks. Virtually all maintenance is done hands-on, on site, by GISI personnel. Whatever little is done remotely is done through SSH secure shell access and only when absolutely necessary. If outside contractors perform any maintenance, they are accompanied by the appropriate SA/NA during the time that they are working on the system.

New servers and workstations are built to comply with specifications and settings provided by IA. Unnecessary services are turned off and unnecessary ports are closed.

**B. Discussion:**

As has been true in other areas addressed in this report, the individual Operations Branch members' SOPs vary greatly in their degree of specificity on maintenance procedures. Similarly, the degree to which the maintenance is documented also varies.

In general, however, all SA/NA personnel are competent and conscientious and conduct routine maintenance in accordance with manufacturers' recommendations. In addition, GISI Operations Branch has an SOP for dealing with vulnerability alerts and individual SA/NA personnel monitor manufacturer and CERT sites to ensure that they remain informed. The Operations Branch has a test lab where patches and other software can be tested before being applied to production systems. After several years of struggling to find opportunities to "fit in" maintenance activities, the IT Division has established a schedule of regular maintenance weekends occurring roughly every fourth weekend throughout the year. The schedule is published to the worldwide GISI community well in advance so that they can make arrangements to be without headquarters' network services during these times. This has greatly improved the up-to-date status of maintenance on GISI IT equipment.

However, for the most part, maintenance activities are poorly documented. Brinkman and Roubieu make a strong argument for keeping an inventory of all computer equipment, including data related to acquisition, identification, usage, and all maintenance activities. "A record should be kept of the maintenance work performed on each piece of equipment, including in-house maintenance and security checks. This information should be available in a central location.....Security is a major concern when dealing with computers ... and the maintenance log is a logical location to record virus checks and clean-ups" (2001, p. 77).

**C. Recommendation:**

1. In conjunction with IA, determine what the SSAA is for each piece of network equipment and what manner of maintenance is needed to remain in agreement with each SSAA.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2. Modify/augment existing SOPs to include all appropriate maintenance procedures for each piece of network equipment and ensure that all SA/NA comply with those SOPs.
3. Develop a consistent branch-wide procedure for documenting maintenance activities. Ensure maintenance logs are stored in a common location and available to all authorized personnel.

**(12) Configuration Management**

**A. Finding:**

The IAPM makes only passing reference to Configuration Management, indicating, "The SA shall maintain comprehensive installation and configuration documentation of the systems under his or her direct control and provide related CM functions" (p. 17). GISI is currently in the process of establishing a configuration management baseline as part of the DITSCAP.

There is no official policy giving IT the authority to maintain control over users' desktop configurations.

GISI does not have a Configuration Control Board.

**B. Discussion:**

Recently there have been improvements in GISI headquarters' approach to configuration management. A single individual is responsible for collecting and maintaining configuration data on all of the headquarters' servers and network equipment. Already the CIO must approve all changes to GISI systems and their configurations; however, in the future SAs will also have to receive permission from the designated configuration manager (CM) before performing updates or other changes to configurations. The CM, in turn, will be responsible for recording those changes and ensuring that up-to-date configuration information is maintained in a central, onsite location as well as offsite. This information will include current system diagrams and a list of all system resources including their location and configuration.

The ability for IT Operations to control the configuration of users' desktop computers is dependent on the Director, GISI implementing a policy giving them the authority to do so. To date, that policy memorandum has not been signed. Nonetheless, IT steadfastly maintains that it is important that users not modify the settings on their computers or install any unauthorized software on their systems (as many GISI users formerly were wont to do). In support of this configuration management objective, when the IT division conducted a "sneaker net" some nine months ago to eliminate a virus that had been accidentally installed by a user and was being spread through the network, the users' workstations were standardized, and the users themselves removed from the local administrators group, the name and password of the local administrator account changed, and a number of pieces of non-standard software removed. In addition, the IT Division has obtained software that will allow it to automatically inventory all workstations so that, in the future, changes to the uniform configuration can be detected and corrected.

The IT Division has a procedure in place for users to request the installation of non-standard software when such software is needed for their job duties. Prior to approval and installation, a member of the Operations Branch checks to be sure the software is legally owned/licensed by GISI, and that the requestor's supervisor deems it

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

necessary. IT then tests the software on a “clean machine” to ensure that it poses no threat to the workstation or the network. Following a successful test, a member of the IT Division installs the software on the user’s workstation.

**C. Recommendation:**

1. Continue to work with the Director, GISI to obtain an Administrative Instruction establishing the CIO’s authority to control the configuration of all GISI computer equipment.
2. Educate the user community on the hazards of installing unauthorized software and ensure that they know how to request non-standard software evaluation and installation where the software is needed to accomplish their duties.
3. Continue to develop and maintain procedures for configuration management of all GISI equipment.
4. Conduct periodic verifications to determine that no unauthorized changes have been made to workstations or other hardware/software.

**(13) Back-ups**

**A. Finding:**

GISI has a comprehensive backup policy and implementing procedures in place. The backups are conducted as scheduled and the ability to restore from backup is tested regularly.

**B. Discussion:**

The IAPM specifies the systems’ backup requirements. It calls for full weekly and differential daily backups of all file and email servers, including both data and system files. It calls for “periodically or as needed” backups of router and switch configuration files to a TFTP server. It also specifies that “Full system backups should precede the installation of major application/services [sic] packages or operating system upgrades.” Finally, it calls for offsite storage of weekly, monthly, quarterly, semi-annual and annual backup tapes (p. 19).

In practice, much of this is well documented and executed, particularly with respect to the Novell and Microsoft servers. Discussions are currently underway to ensure full compliance for all Operations Branch computer equipment and to ensure the record keeping and reporting requirements of the IAPM are complied with.

Current practice is to take monthly full backups of Novell and Windows servers to an offsite location. The most recent month’s backup is kept onsite to facilitate data recovery; the next most recent is stored offsite. This process can be improved if GISI can find an economical way to duplicate backup tapes.

**C. Recommendation:**

1. Determine a method for duplicating backup tapes so that the latest monthly and weekly tapes can be maintained both on- and off-site.
2. Ensure that all server backups (including those of Unix servers) are performed according to the IAPM requirements, including offsite storage of backup tapes.
3. Provide for regular backups of firewall, router, and switch configuration data and for storing copies of that data off-site as well.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**(14) Labeling**

**A. Finding:**

The highest level of information processed at GISI headquarters is sensitive but unclassified (SBU). According to the GISI IAPM, “Unclassified media used solely with SBU systems does not require classification labels” (p. 22).

The Backup section of the IAPM makes no mention of labeling backup tapes; neither does the IT Division memorandum establishing Backup Policy. The Windows NT and Netware Server Backup Administration SOP specifies that “tapes are identified by jobname ... date, and tape serial number.” The Unix System Administrator’s SOP makes no mention of the manner in which backup tapes are labeled.

**B. Discussion:**

NIST 800-12 indicates: “From a security perspective, media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system” (p. 161). This implies that, beyond marking tapes as described in the SOP, GISI should also use labels to identify tapes that contain FERPA or other sensitive information.

**C. Recommendation:**

GISI should develop a unified, comprehensive policy on the labeling of backup tapes and other removable media. The policy should address the sensitivity of the information stored on the tapes and should include specifics as to label content and format. Once developed, this policy should be applied uniformly by all of those responsible for performing backups.

**(15) Media Sanitization/Disposal**

**A. Finding:**

GISI headquarters has a strict policy concerning the disposition of computer hard drives. However, no mention is made in the IAPM or in the various Operations Branch SOPs of the procedure to be followed when backup tapes are taken out of service.

**B. Discussion:**

The GISI IAPM cites four methods of hard drive sanitization and cleaning: overwriting, degaussing, destruction, and clearing (p.22). The IAPM further states that the clearing procedure is to be used when the media will remain within a GISI facility, but that overwriting is required before media can be released outside of GISI custody.

An examination of the Backup Policy and Windows NT and Novell Backup SOP as well as the Unix administrator’s SOP reveals no specific instructions on the handling of storage tapes that are taken out of service. Interviews with Operations personnel reveal that the tapes are currently being stored in the fireproof safe in the server room.

**C. Recommendation:**

Establish a specific policy for dealing with magnetic storage tapes that are taken out of service. Educate Operations Branch personnel as to the provisions of this policy and incorporate the policy into Backup Administrators SOPs.

**(16) Physical Environment**

**A. Finding:**

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

GISI headquarters' servers and LAN/WAN equipment are stored in a secure, climate controlled location in the interior of the building. Access to equipment is restricted and controlled.

**B. Discussion:**

Physical access control to the headquarters facility is accomplished through proximity badges issued to GISI employees and their contractors possessing valid GISI issued CAC cards with photo ID. Facility access granted by the proximity badge is refined according to the needs of the employee, varying from access to only one floor, only between 8 AM and 5 PM Monday through Friday, to access to all floors, 24 hours a day, seven days a week. Security cameras monitor the doors leading from public spaces into GISI controlled spaces and the proximity badge system records the time and identity of each employee's access.

Visitors who are government employees and possess valid photo ID are issued badges indicating no escort is required; all other visitors are issued an escort-required badge. Access to the server room is restricted to members of the IT Operations Branch, and access to the wiring closets is controlled by limited key distribution.

These protective measures are only as strong as the vigilance of the employees' practice of them. It is not unusual to observe individuals inside the facility who are not displaying either an identity badge or a visitor's badge. Only rarely are these individuals questioned as to their status. It is also quite common for one employee in the company of another to pass through an entry point without using his/her own proximity badge to obtain the access.

**C. Recommendation:**

The security of the physical environment can be improved through more thorough application by employees of the existing protective measures. (See "Training and Awareness" section of this report.)

**(17) Personnel Security**

**A. Finding:**

GISI systems administrators and network administrators are all American citizens and have been given background checks. GISI does not process classified information, so there is no need for security clearances for IT personnel.

All users sign a Computer and Internet Access Agreement before they are given access to GISI computer resources.

Interviews revealed that GISI users have little or no awareness of the hazards to GISI computer systems from inside the network. They have no knowledge of social engineering techniques. Many share their passwords with other users and/or with their supervisors; for them most part they do not use strong passwords and in some cases they keep a written copy of their password in an obvious location. Administrators do not always know when users have left GISI; hence some accounts remain active longer than they should. All of these facts place the network at risk for attack from the inside.

**B. Discussion:**

Users' security awareness is low and needs to be improved (see "Training and Awareness" section of this report).

Communications with the Personnel Division regarding departing employees also need to be improved. (See "Account Management" section of this report)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Although all SA/NA personnel have been given background checks, GISI would be well served by conducting periodic rechecks.

**C. Recommendation:**

1. Conduct formal Information Security training for all new users; conduct periodic INFOSEC Awareness campaigns for all users. In both cases emphasize the dangers of system compromise from the inside.
2. Arrange with the Personnel Division to receive weekly reports of employees leaving GISI and ensure that their accounts are immediately disabled or deleted.
3. Conduct periodic background checks on all computer network personnel.
4. Ensure that all SA/NA personnel update their security awareness on an annual basis. Consider requiring that all SA/NA obtain the Security Certified Network Professional (SCNP) or other equivalent certification.

**(18) Training and Awareness**

**A. Finding:**

The GISI IAPM clearly calls for a Security Training and Awareness Program for all GISI users and systems administrators. The program's implementation, however, leaves considerable room for improvement.

**B. Discussion:**

The GISI Information Assurance Program Manual (IAPM) clearly establishes the need for a Security Training and Awareness Program. It requires that all users of GISI information systems participate in an initial security briefing and a yearly INFOSEC awareness training session. The content of the training is found on a CD made accessible to users on the GISI network. Each user's desktop has a shortcut to the training material. At the end of the training, the user can print a certificate indicating completion of the training.

In October 2001, when the training material was originally put in place, an email to the user community informed them of the training requirement and the fact that they were to view the training, print the certificate, and turn in a copy to IA. Since that time, there has been no further publicity regarding the requirement; neither has there been follow up with users who have not completed the training. There is no mechanism in place for informing new employees of the training.

According to Susan Hansche, writing in the January/February 2001 issue of *Information Systems Security* journal, "Various computer crime statistics show that the threat from insiders ranges from 65 to 90 percent [of all threats to the system]." Although the GISI program meets the letter of the law (Computer Security Act of 1987) and satisfies the requirement to provide security awareness information to all end users of information systems (Hansche, 2001a), in its current state of application, it is not an effective program for mitigating the risk of attack, inadvertent or otherwise, from inside the GISI headquarters' system.

**C. Recommendation:**

Before putting the following three recommendations into effect, the ISSM should conduct a briefing for management at all levels, informing them of the importance of protecting GISI information and systems from inside attack as well as the role of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

INFOSEC Awareness and Training in accomplishing that objective. Once upper management support for the program is present:

1. Initiate a security awareness campaign, using such vehicles as pop-up announcements, email "security message of the day" explanations and factoids, and eye-catching posters to raise all employees' consciousness and "heighten the importance of information systems security and the possible negative effects of a security breach or failure" (Hansche, 2001a).
2. Initiate a half-day training session for all new employees during which the specifics of GISI's security policies and practices can be reviewed and, where appropriate, practiced or role-played by participants. This training session should also address the concerns regarding Physical Security. (See "Physical Environment" section of this report). It may be possible to combine security awareness training with the newly initiated half day training in Mailbox Management that is now required of all new employees.
3. Make better use of the existing security awareness training program, verifying that employees meet the annual training requirement and following up with those who fail to do so.

Note: Hansche's three journal articles expound on the framework established in NIST SP 800-16 "IT Security Training Requirements: A Role- and Performance-Based Model". The third of her articles, found in the July/August issue of *Information Systems Security* is an updated version of her March/April article of the same name. The July/August version, however, is considerably expanded and contains valuable appendices detailing specific course outlines predicated on employees' roles and responsibilities within the organization.

**(19) Risk Assessment** *(At the request of the customer, this category is added to the 18 defined within the IAM.)*

**A. Finding:**

GISI recently conducted a Network Security Testing and Evaluation (ST&E) in order to assess the risk to its network and resources posed by vulnerabilities discovered. SA/NA personnel are currently evaluating the ST&E findings and mitigating vulnerabilities discovered through the ST&E.

**B. Discussion:**

The ST&E, conducted by an outside consultant, appears to have been almost exclusively a penetration test conducted from inside the GISI network against GISI provided IP addresses. Viewed from that perspective, it should be seen as only a start at assessing GISI's risk from attack. It provides valuable information to GISI SAs who are currently studying the test results to determine which vulnerabilities should be fixed and which they will recommend the CIO accept as residual risks.

Peter Stephenson points out that the reason for testing is "to learn what we need to do to strengthen the security of the overall system. To do that, we need to know what's on the network, perform broad, comprehensive tests; fix what we find; test again, and then, if we really want to be sure, use a penetration team to QA our work" (2000, p. 6). While the current ST&E provides some understanding of the vulnerabilities that exist on GISI workstations and servers, a broader based test is needed to determine vulnerabilities that may exist on servers in the DMZ and on firewalls and routers and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

switches connecting the servers and workstations both to each other and to the outside world.

The GISI IAPM states: “An integral part of the DITSCAP process is the evaluation, mitigation, and management of risk. GISI systems administrators must adequately address a system’s susceptibility to exploitation, the potential rewards to exploiters, and the probability of such an occurrence or any related threat. They should be prepared to document the residual risk, i.e., that portion of the risk that remains after the security measures have been applied” (p. 12). When GISI SAs have finished mitigating and/or accepting the risks due to the vulnerabilities that the ST&E has identified, they will need to look elsewhere to fulfill their IAPM imposed charter of “adequately address[ing] ... system’s susceptibility to exploitation.” As Stephenson goes on to point out, “We want to identify and offer a corrective action for every vulnerability on the system. That means network vulnerabilities, host vulnerabilities, server vulnerabilities, and internetworking device vulnerabilities” (Stephenson, 2000, p. 8). His article recommends a number of commercial tools that may be useful to GISI in conducting the broader vulnerability assessment.

Finally, Stephenson also points out that a network’s vulnerability goes beyond those things that are discovered through vulnerability or penetration testing alone. He suggests that following the Central Intelligence Agency’s classic definition of security as confidentiality, integrity, and availability, an extremely slow network can be considered a vulnerability, as can the lack of a configuration management program. The risks associated with these and other factors that are not typically considered “vulnerabilities” should be considered as well and should be remediated to the extent possible.

**C. Recommendation:**

1. Apply corrective action to the vulnerabilities identified by the ST&E, except where to do so is not possible or would cause an unacceptable loss of functionality. In cases where remedies are not applied, document the rationale and offer a recommendation for accepting the residual risk. Where appropriate, ensure that policies are more rigorously applied in order to prevent reoccurrence of these same vulnerabilities.
2. Conduct a second round of testing to ensure that the identified vulnerabilities have been removed and/or documented as accepted risks.
3. Conduct similar testing on those servers and devices that were not covered in the ST&E in order to discover and either remedy or accept their vulnerabilities.
4. Repeat the overall vulnerability assessment process at least every six months.
5. Continually ask: “What else poses a potential risk to the confidentiality, integrity, availability, authentication and non-repudiation aspects of the GISI system and what can we do to mitigate those risks?”

## CONCLUSION

On the whole, GISI is well on its way to developing a strong information security (INFOSEC) posture. The present INFOSEC analysis reveals strength in the areas of INFOSEC Documentation, particularly the Information Assurance Program Manual and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

several of the Operations Branch Standard Operating Procedures. A number of basic INFOSEC policies are already in place and several others have been prepared and are merely awaiting the director's signature. In addition, GISI's network security posture has been well planned and its equipment is properly configured for maximum protection of its valuable assets. Extensive provision (HA firewalls, backup telecommunications lines, quick response maintenance contracts, etc.) has been made to ensure maximum protection for the users' access to network resources.

We encourage GISI to continue its progress in the areas of configuration management and account management and to continue its practice of conducting and responding to risk assessments.

GISI can significantly improve its INFOSEC posture by taking action on the recommendations in the enclosed report, particularly those on Training and Awareness for all end users and the development of a strong Continuity of Operations plan. Although INFOSEC roles and responsibilities are clearly defined, there is a need to better communicate some of their responsibilities to the Operations staff charged with fulfilling them.

Considering the potential loss to GISI headquarters' primary mission of supporting the schools should the headquarters' network suffer extended downtime, it is easy to appreciate the importance of investing in protecting that network from INFOSEC threats and vulnerabilities, and to see that the time, effort and dollars invested in improving GISI's INFOSEC posture and protecting against down time are being well spent. Moreover, the easily quantifiable personnel costs associated with lost productivity should the headquarters' network suffer prolonged down time can be readily balanced against the personnel and equipment costs associated with ensuring against such network outages.

The recommendations contained in this assessment are suggested guidelines for improving GISI's INFOSEC posture. They are not requirements and the implementation of any of the recommendations is solely at GISI's discretion.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Allan, Ant. (March 7, 2002). “Authentication: Perspective”. URL: http://www.gartner.com (January 19, 2003).

Avolio, Fred and Piscitello, David. (May 2001). “E-Mail Security – Signed, Sealed & Delivered”. Information Systems Security, 10 (2). URL: http://www.infosecuritymag.com/articles/may01/features_email_security.shtml (13 March 2003)

Brinkman, Carol S. and Roubieu, Amanda M. (2001). “Planning and Record Keeping for Computer Maintenance and Management”. Reference Services Review 29 (1) pp. 72-80.

Corbitt, Terry. (May 2002). “Protect Your Computer System With a Security Policy”. Management Services, 46 (5) pp. 20-21.

Digital Knowledge. “National Security Agency INFOSEC Assessment Methodology”. URL: http://www.digitalknowledge.net/dk/s_nsaiam.asp (January 23, 2003).

Hansche, Susan. (January/February 2001). “Designing A Security Awareness Program: Part I”. Information Systems Security, 9(6) pp. 14-21.

Hansche, Susan. (March/April 2001). “Information System Security Training: Making It Happen: Part 2 of 2”. Information Systems Security, 10(1) pp. 48-56.

Hansche, Susan. (July/August 2001). “Information System Security Training: Making It Happen: Part 2”. Information Systems Security, 10(3) pp. 51-71.

Hoffman, Mark A. (October 23, 2000). “Business Continuity Plans Need Constant Refining”. Business Insurance 34 (43) pp. 67-68.

The International Information Security Foundation ($I^2SF$)-Sponsored Committee to Develop and Promulgate Generally Accepted System Security Principles. (Fall99) “Generally Accepted System Security Principles (GASSP) version 2.0”. Information Systems Security, 8 (3) pp. 32-51.

Kleckner, James E. (May/Jun 2002). “E-security 101”. AFP Exchange, 22 (3) pp. 54-56.

National Institute of Standards and Technology. “NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook”. (March 1996) URL: http://cs-www.ncsl.nist.gov/publications/nistpubs/800-12/ (15 March 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

National Institute of Standards and Technology. “NIST SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model”. (April 1998). URL: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (15 March 2003).

National Security Agency (NSA). “INFOSEC Assessment Training and Rating Program”. URL: http://www.iatrp.com/pdfs/categories_3.pdf (13 March 2003)

National Security Agency (NSA). “INFOSEC Assessment Training and Rating Program”. URL: http://www.iatrp.com/pdfs/IAM-Module-2.pdf , pp. 29-38 (13 March 2003).

Oar, Gerald L. and Jackson, Robert H. “The Benefits of Applying the DoD Information Technology Security Certification and Accreditation Process to Commercial Systems and Applications”. (October 1998). URL: http://csrc.nist.gov/nissc/1998/proceedings/paperE2.pdf (15 March 2003).

Phillips, Andrew. (January 14, 2002). “Enterprise Smart Cards: Securing Buildings, PCs and Corporate Networks”. URL: http://www.gartner.com (January 19, 2003).

“Presidential Decision Directive/NSC-63”. May 22, 1998. URL: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (24 January 2003)

Robb, Drew. (April 2002). “Protecting Sensitive Data Requires Vigilance”. HR Magazine 47 (4) pp. 91-96.

Stephenson, Peter. (Mar/Apr 2000). “Assessing Vulnerabilities”. Information Systems Security 9 (1) pp. 5-9.

United States Department of Education. “Family Educational Rights and Privacy Act”. URL: http://www.ed.gov/offices/OM/fpco/ferpa/index.html (15 March 2003).

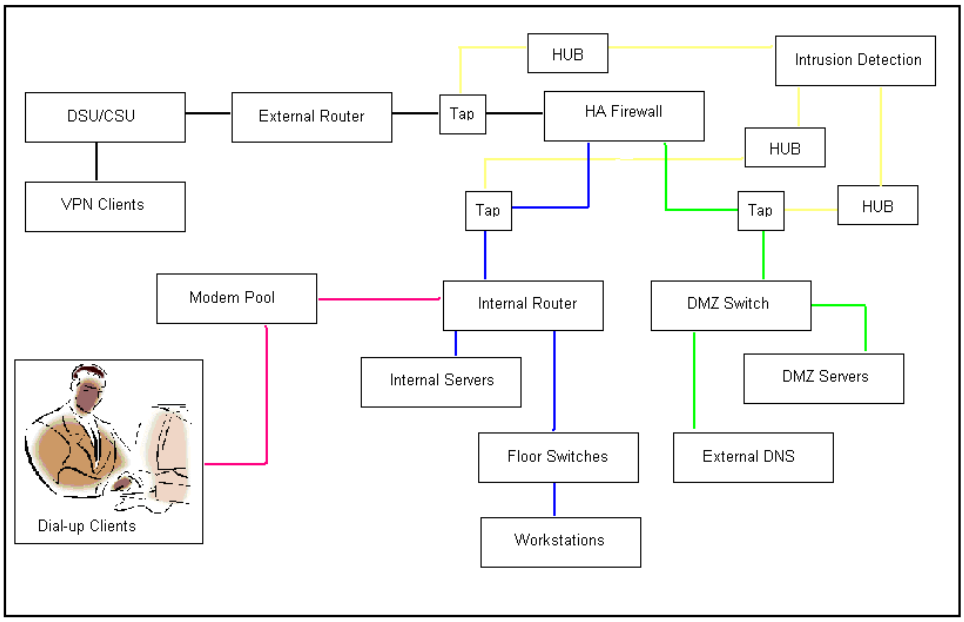
Wojcik, Joanne. (April 29, 2002). Continuity Management Requires Commitment. *Business Insurance 36* (17) p. 18.

Woosley, Lynn. (October-December 2002). Careful Contingency Planning Can Save the Day. *Financial Update* 15 (4) pp.1-2.

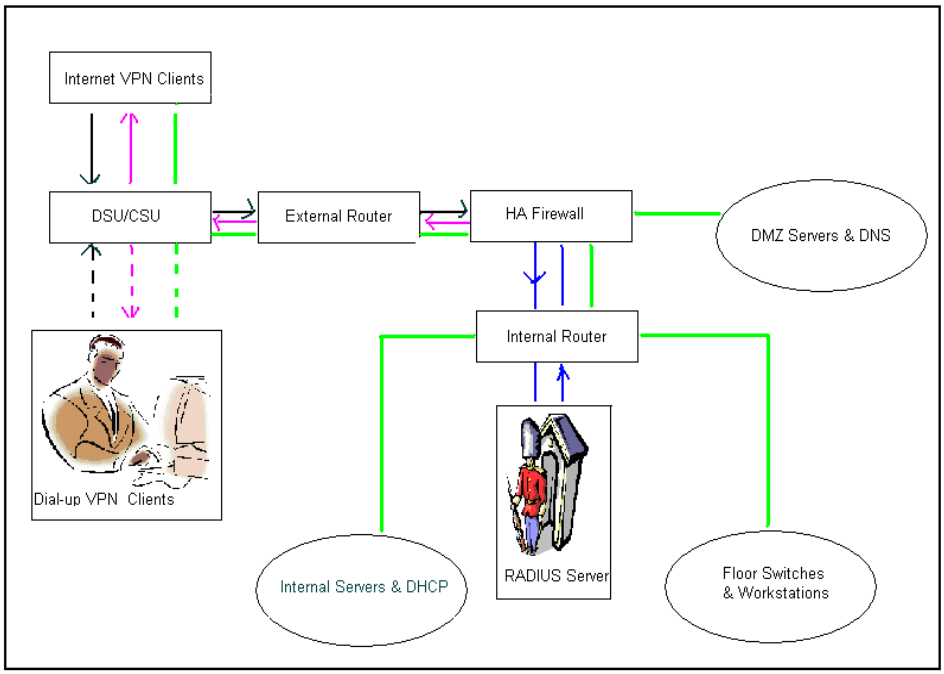
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## APPENDIX A – SYSTEM DIAGRAMS

GISI Network and Telecommunications Infrastructure




Proposed Modifications to GISI Network and Telecommunications Infrastructure




© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## APPENDIX B – DOCUMENTS REVIEWED

The following documents are pertinent to GISI Information Security and were reviewed during the course of this assessment.

| | |
|---|---|
| DoD Instruction 5200.40 | DoD Information Technology Security Certification and Accreditation Process (DITSCAP) |
| GISI Instruction 6700.5 | GISI Information Assurance Program Manual |
| GISI Instruction 6700.8 | Computer Audit Trails |
| GISI Instruction 1060.1 | WWW Site Administration |
| GISI Instruction 6700.2 | Computer Software Piracy |
| GISI Regulation 1400.0 | Electronic Mail System |
| GISI Policy Memorandum | Continuity of Operations |
| GISI Policy Memorandum | DITSCAP |
| GISI Policy Memorandum | Computer Network Defense |
| GISI Policy Memorandum | Configuration Management |
| GISI Policy Memorandum | Designated Approving Authority |
| GISI Information Technology (IT) | Backup Policy Memorandum |
| GISI IT Operations | Backup Standard Operating Procedure (SOP) |
| GISI IT Operations | Local Area Network (LAN) SOP |
| GISI IT Operations | Unix System Administrator (SA) SOP |
| GISI IT Operations | Novell SA SOP |
| GISI IT Operations | Electronic Mail SA SOP |
| GISI IT Operations | IA Vulnerability Alert (IAVA) SOP |

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## APPENDIX C – Individuals and Positions Interviewed

The following individuals are pertinent to GISI Information Security and were interviewed during the course of this assessment.

| | |
|---|---|
| Associate Director for Management | |
| Associate Director for Education | |
| Chief Information Officer | |
| ISSM | |
| ISSO | |
| Chief of Security | |
| IT Chief of Operations | |
| Email System Administrator | |
| Backup Administrator | |
| Novell System Administrator | |
| Unix System Administrator | |
| Database Administrator | |
| Configuration Manager | |
| Firewall Administrator | |

© SANS Institute 2003, Author retains full rights.