Global Information Assurance Certification Paper

GIAC Enterprises
Standard Operating Procedures
& Security Policies

Revised Submission dated 26 Feb 2002

GISO Practical Assignment
Version 1.1 (December 12, 2001)

TABLE OF CONTENTS

Assignment-1: Description of GIAC Enterprises

Business Description:

GIAC Enterprises is a joint venture higher learning institution catering to federal government education in applied mathematics and sciences. It functions in cooperation with several prime contractors that provide technical and developmental services for educational matter, format and presentation. The primary learning center is contained in a single campus structure with self-contained support facilities. Prime contractor locations are various across the contiguous United States and are connected to GIAC Enterprises via a dedicated switching network using encrypted ATM circuits.

The company staff of approximately 500 is predominated by instructors along with associated support personnel including administrative, physical security, legal, information systems and technology (IS&T.) The company's primary focus is student training which centers on the implementation of streaming multimedia and menu driven applications both in the classroom and independent learning resource centers (LRC) housed within the campus proper. Company profit is measured in continuity of "up time" and on-time development of continuing training topics. These functions are directly supported by in-house multimedia development teams in conjunction with local and remote contractors.

IT Infrastructure:

GIAC Enterprises operates in a mixed environment predominated by the Microsoft Windows NT4.0 (NT4) operating system (OS.) One server exists with the Novell Netware 5.1 OS running GroupWise in order to connect via encrypted communications to several prime contractors at remote locations. One additional Unix based print server exists internal to a Sun workstation supporting high volume document preparation and lithographic services.

Several distinct networks exist to provide services for material categorized as follows:

1. Government classified information,
2. Encrypted traffic segment for communicating with the prime contractors,
3. General purpose demilitarized zone (DMZ,)
4. Multimedia development and production,
5. A student learning resource oriented segment (located inside the DMZ.)

Each network is physically separated in distinct physical racks and labeled for clarity including separate wiring colors and media to readily identify its usage as shown in Appendix-A. All servers are centrally located in a secured server room along with core switching devices from Cisco including PIX 515 Firewalls, 1900, 2900, and 5505 series Switches (one containing a router module,) and 3600 series routers with IP packet filtering. Additional media converters are provided to convert the backbone fiber network to Category-5e UTP copper. All data travels over fiber within the primary distribution nodes and is converted to copper media at key switching closets that support department level nodes within the campus building. A single ATM concentrator coupled with a multiplexer and encryption unit provides secure communications via a dedicated circuit to key contractors off-site using proprietary hardware and software. (For the purposes of this paper, the specifics of encryption equipment may not be

detailed.) The network is segmented to provide classification boundaries meeting government requirements to minimize unnecessary classification of information. Based on existing security policies published by GIAC's DAA and prime contractors, once documents are moved into the classified network, they should not be declassified for transfer unless scanned with proprietary scanning software. In addition, the currently acceptable file formats for declassification scans are limited to text (.txt), rich text (.rtf), hypertext (.html), ASCII comma delimited text, file interchange format graphics (JPG, JPEG), bitmap graphics (BMP), or graphical interchange format (GIF). This is an externally generated policy and may not be changed at GIAC. Therefore, all activities that do not expressly require classification are conducted on the unclassified segment inside the DMZ, and all work requiring future classification is conducted on the multimedia development or classified segments. The control of classified transfers to the prime contractors is controlled by routing rules through the classified Proxy server, the VIP2 RSM of the Cisco 5505, and onto the network segment reserved for encrypting/decrypting information for transfer off-site. These transfers are limited to key personnel with appropriate user rights specific to communications security.

1. Classified Segment:

This segment of the network hosts the portions of the overall network dealing with government classified information including final classroom presentation material. All finalized lessons and presentation material are stored on a hardened Dell 1550 series server provided for file access purposes. Multimedia presentations are pushed down to local workstations in each classroom by a technician. From these local stations, the multimedia lessons are presented via projector and sound systems. A separate PDC, BDC, and print server are provided for authentication to access and print classified material. These are also hardened Dell 1550 series servers. The Oracle database is located on a hardened Dell 4400 series server and hosts numerous activities. The primary purpose for Oracle includes hosting exam bank storage, student academic records, building access control logs generated by badge readers throughout the complex, and staff continuing training information. The final server in this segment is a hardened Dell 4400 hosting MS Proxy services and software IDS to control access into and out of the network segment. This allows better control of rule sets and traffic flow. All servers run client installations of Symantec Corporate Edition antivirus software. The BDC also hosts the segment Exchange post office for Intranet e-mail.

2. Encrypted Traffic:

The encrypted segment as shown in Appendix-1 Network Diagram comes off of a Cisco 5505 switch with a VIP2 Route Switch Module (RSM) to allow direction of data to and from the classified network and multimedia development segments. The host server is a Dell 2300 running Novell 5.0 NOS that directs messages and data traffic through the encryption device and ATM circuit to and from the prime contractors. The primary data transferred includes student record information, multimedia lessons in their developmental stages, and message traffic between contractors and GIAC staff using GroupWise. Information is pushed from the Oracle database to servers at the various prime contractors for update purposes only.

3. General Purpose and DMZ:
This segment of the network represents the access point to and from GIAC with the Internet. This access point is provided for several purposes including a locally hosted web page with general information about GIAC and its educational purposes. Additionally, it provides the connection point from the LRC and internal network segments for access to Internet resources. It provides the first line of defense using a Cisco PIX 515 firewall connected to a hardened Dell 4400 running MS Proxy and software IDS. Traffic is filtered and routed via a Cisco 5505 switch to the DMZ PDC for unclassified general use access and authentication. The PDC, BDC, Exchange, and IIS servers are all Dell 1550 series and each server runs Symantec Corporate Edition antivirus software. E-mail services are provided for students and staff alike in this segment and therefore policy forbids the use of personal web-based e-mail.

4. Multimedia Development:
This segment of the network hosts several development workstations, a rendering farm for graphics and animation production, and a Proxy server for traffic control. This segment of the network is considered government classified since it hosts the development of lessons relating to classified material. The Proxy server is a Dell 1550, and the render farm consists of forty high-end workstations. All computers run Symantec Corporate Edition antivirus software. The primary purpose for this segment is the development of multimedia lesson plans and teaching tools to support the primary mission of GIAC as a learning institution. Periodically, lessons are sent via encrypted traffic to prime contractors for content and context evaluation. Once evaluated and modified by contractors, these finalized plans are returned through encrypted traffic to the classified network segment for management review, acceptance, and storage for instructor use.

5. Student Learning Resource Center (LRC):
This portion of the network resides inside the DMZ for the purposes of providing general study resources for students and for e-mail/Internet access. These study materials and utilities are not classified in any manner and therefore should reside on a network segment with the lowest government security classification. This network resides inside the logical DMZ since it is the only available segment with a "lowest level" classification and allows Internet access through the Proxy server.

All workstations are x86 based Intel machines, most provided by Dell. Five different types of configurations exist due to the current phased replacement cycle. All run NT4 workstation with SP6a and the post-6a roll-up pack installed. In addition, applicable hot fixes are installed as delineated in Table-1 of Appendix-B.

The current network plan includes a migration to the Windows 2000 OS in the third quarter of this year. This will include migrating all server software to the 2000 equivalent, and the Oracle database from 8.16 to 9i. Security enhancements native to each application and better multimedia support coupled with plug-and-play features will improve the network and company ability to provide future product improvements and better training.

Business Operations:
The company's central IT needs are based around the primary mission of providing high quality, cutting edge multimedia training. As such, the proposed Win2K OS upgrade will allow more graphically enhanced presentations using such software as Visio, Authorware, Flash, Java, 3D Studio Max, and others. This paper will focus on the critical needs surrounding development and handling of training lessons and student data since this involves the creation, warehousing, and periodic transmission of government classified data. The company requires continuous operation of several central applications in the following decreasing priority:

- 100% up-time on the presentation computers in each lecture/class room during normal business hours.
- 100% availability for Render Farm equipment and associated developer workstations.
- 100% Oracle availability during at all times for in-house and external data synchronization

To achieve these goals, GIAC Enterprises relies upon a multi-layered strategy of defense in depth coupled with redundancy in systems, application availability, and data storage. As an example, if a permanently installed classroom computer system fails, mobile carts with identical configurations are available. The goal is to ensure no IT system failure causes greater than a five-minute delay in lesson presentation time.

In the realm of multimedia development, the majority of work is performed locally with approval authority residing with two prime contractors off-site. Typically this involves developing lesson plans with associated graphics and action media, then sending this product via encrypted traffic off-site for review and comment. Once final review is complete, an editorial change request is returned via encrypted traffic for local developers to take action on. After final local approval of the curriculum, it is pushed onto the academic portion of the classified network for distribution to classrooms. Updates are conducted through one-way pushes from the central servers using batch jobs that place the appropriate curriculum onto classroom presentation machines based on teaching schedules housed in Oracle and running under a scheduler service.

The Oracle server and database host much of the administrative activities of the company. Everything from human resources information to the classified exam banks is housed here. In addition, student and staff physical access to the LRCs and campus proper are controlled via a badge identification system to account for building and resource use, as well as to ensure limited access to sensitive areas such as the server vault. In the event that the system is down, local hand-held wanding stations are available to log people in and out of the complex. The database is also used for pushing training progress updates and student information to the prime contractor.

The intranet services of all LAN segments are important to the daily operation of the company since this aspect of the network supplies access to company information, policies, operational commitments, and interoffice communications. Two e-mail systems exist; one based on Microsoft Outlook, and the other on Novell GroupWise. The latter is used exclusively with the prime contractors and is limited to senior staff and developers. External e-mail is routed in accordance with rule sets at the firewalls, routers, and Proxy servers and is scanned three times

with corporate edition antivirus software. A series of successively restrictive rule sets remove attachments by type as information is routed deeper into the network.

The LRCs are used almost exclusively by students in their early phases of program study with subject material ranging from interactive mathematics programs to basic engineering analysis. Laboratory access is available from mid afternoon until the building closes at midnight each business day. None of the courseware is available for external access at this time due to proprietary development restrictions. However, students do have Internet access from the LRC machines and may use locally hosted e-mail services. No web-based e-mail or chat is allowed since it is harder to secure and poses a conflict with the primary purpose of the LRC as a study center. Physical access to the LRCs is controlled via badge readers and is monitored by closed circuit TV to ensure appropriate personal conduct and as a back up to network monitoring efforts.

There are no telecommuters at the current time; therefore, no RAS or equivalent services are necessary. In addition, remote site access via the Novell systems is limited to data transfers and does not include live software or application manipulation through the encrypted circuit. However, digital teleconferencing does exist over the encrypted circuit hosting meetings with several off-site contractors.

In addition to previously stated software, the company relies upon the MS-Office 2000 Premium suite, MS Back Office suite, Veritas Backup Exec, Symantec Corporate Edition virus software, and proprietary implementations of software IDS. It is the responsibility of IS&T to both deploy and provide user assistance on all software hosted on the various networks.

(End Assingment-1)

Assignment-2: Definition of Security Policy

Areas of Risk:

Stephen Fried defines risk as "a potential for loss or harm . . .[that] usually comes about because you have a vulnerability to some sort of threat." Since GIAC's primary mission includes the development and handling of classified documents and their presentation and storage, some potential threats include theft, defacement, loss of data validity, and loss of trust for handling special material.

Five key areas of the Company's network security will be examined:

1. Encrypted Network Traffic

Reasons for concern – The Company's encrypted network traffic is critical to the successful development of topical lessons and is central to the overall mission of training. Developmental stage lessons are moved from the multimedia segment of the network through the VIP2 RSM to the Novell server and prepared for encrypted transmission. Improper transfer of information could result in classified data being misplaced on the network, or improper encryption prior to transmission. In either case, this constitutes mishandling of sensitive information that could lead to loss of trust, reputation, and potential loss of data validity.

Perceived Threats and Consequences – The primary concern is electronic handling of sensitive data from the source server store to the Novell server, encryption and transmission. In addition, improper maintenance and synchronization of encryption keys could potentially cause self-inflicted denials of service, or unintentional exposure of insufficiently encrypted information.

A break in encryption could expose the system to the introduction of malware/spyware with the intent to harvest key codes, passwords, unprotected data stores, or to destroy data on exposed systems. The loss of control over certain proprietary data could result in prosecution under federally mandated restrictions on information dissemination.

A loss of student or staff data during transfers could lead to a loss of privacy and may expose GIAC to prosecution under the Privacy Act of 1974 if negligence were shown.

Mitigation – The primary method of preventing compromise lies within the procedures and training surrounding communications security. All personnel associated with ComSec are required to have appropriate clearances and participate in quarterly refresher training. In addition, by requiring the use of procedural check sheets that outline a step-by-step process

for the handling of classified information from inception to final destination, formality and due care are more assured.

The next layer to InfoSec/ComSec is limiting physical access to the requisite servers and encryption equipment. All classified servers are housed in a vault requiring logged access and combinations for entry. By placing encryption equipment inside a two-lock safe located in the server vault, and requiring a two-person policy for access to encryption keys and hardware, a single point failure is significantly reduced. Since access to these areas is logged into the Oracle database, a formal method of tracking prevents accidental exposure of the affected systems.

Protecting encryption keys includes limiting physical access as described above, as well as by rotating key codes on a regular basis. Through diligent handling procedures, the likelihood of compromising encryption codes is reduced.

Finally, the network design ensures that data transfer is limited to local machines inside the server vault preventing remote transfers that could go awry. The proper use of transfer procedures, personnel screening and training, and layered defense in switching gear helps ensure proper routing of information between the classified networks and the encryption server.

Implementation Costs – Several areas contribute to the overall cost of implementation.

The greatest initial cost is requiring security clearances for a limited number of key custodians. Current estimates place these clearances at approximately $80,000 apiece and should be initiated sparingly. Proper planning is required due to the long lead-time in acquiring the appropriate level for cryptographic equipment and compartmentalized information handling.

Additional personnel assigned to the specific tasks of key code encryption, and maintenance of equipment, increases the size of the IS&T department since the primary and secondary custodians should have no other duties to prevent any one person from having full LAN access. This increase in personnel also raises associated HR costs.

The necessary equipment to provide key code encryption and data scrambling is very expensive not only to purchase, but also to acquire licensing and accreditation for; therefore, a long term phased replacement strategy and careful handling must be adhered to.

Finally, the cost of rotating key codes and reprogramming equipment causes down time for that portion of the network requiring adequate company wide notice and scheduling to prevent conflicts with critical data transfers.

2. Limited Physical Access

Reasons for concern – The building used by GIAC is cleared for classified material storage and conversations and therefore must have limitations on who may enter the facilities and

under what conditions they may enter. Allowing uncleared people to enter sensitive areas could compromise the control of sensitive information, and could lead to a loss of trust or professional reputation. While all staff and students at GIAC have access to the building, there must be layers of limited access to the various departments based on a need-to-know. As an example, allowing students to have access to multimedia development areas could seriously compromise the integrity of exams. Another example would be allowing basic instructors access to the servers. In each case, data validity could be compromised, or the network security compromised if knowledgeable intrusion efforts were attempted.

Perceived Threats and Consequences – The Company employs people in various job descriptions, but only 60% of the business actually needs access to training information, development software, and examination banks. The remainder provides physical security and administrative functions unrelated to training.

The building is designed with a badge reader system linked to the central Oracle databases where levels of access rights are assigned based on grouped job descriptions. Students are allowed general access to the main building, to classrooms, to the LRCs, and to instructor office areas. Administrative staff has access to the main building, general office areas, and boardrooms, but are restricted from teaching classrooms based on a need-to-know. This concept governs access to other areas of the building so that only assigned IS&T personnel may access the server vault or communications closets, and this carries on based on job functions and a demonstrated need to work in portions of the building.

The location of data stores is based on the combination of information security and assurance as described earlier as well as physical access limitations. Servers are physically separated within the vault and clearly labeled for use and classification level. Only unclassified information is housed on DMZ machines. Only classified information is stored on the classified servers. Access to the server vault is physically and logically limited to IS&T staff assigned to the roles of network administration, maintenance, database administration, information security, and network security management. Students and staff only have physical access to machines in areas of the building they are cleared for, and logical access is controlled across the domains based on group policies and routing rules.

Since staff members with access inside the classified and development networks have varying degrees of access to information and databases, they pose the greatest risk. An incident of inappropriate access could compromise exam security or invalidate lessons due to stolen or altered data and subject personnel to prosecution under federal regulations for restricted information.

Mitigation – Numerous methods can be utilized to ensure a "best effort" approach to information security is followed.

First and foremost – proper training of staff and students with heightened sensitivity to the proper use, handling, and storage of proprietary information. This includes briefings on access control policies, ensuring people know where they are allowed to be, and under what circumstances they may be there.

Second – proper installation of locking devices including cipher door locks, safe locks, badge readers controlling access to spaces, and the deployment of closed circuit monitoring devices in key access ways. Proper monitoring of entry/exit points with recorded media provides deterrence through advertising the fact that activities in the complex are being observed.

Third – implementing physical plant access controls on a need-to-know basis as described above to prevent the accidental exposure of people to information they should not have access to. This includes describing personnel access limitations based on job descriptions, and logically enforcing this through database controlled badge readers.

Finally, proper deployment of security personnel and frequent periodic checks of limited access spaces will mitigate the chances of internal misuse by reducing opportunity.

Implementation Costs – Overall, these methods can become very expensive quickly. Biometrics, real time IDS evaluation, complicated locking systems, and the additional personnel to monitor/respond to incidents raise the bar for entry into business operations. The overall return on investment (ROI) is complicated by balancing the potential loss of proprietary information against continued upgrades necessary to maintain high security. In this case, only the most secure areas may warrant full security measures.

Personnel training ranges from indoctrination to continued periodic refreshers on standing policy. No direct monetary cost is associated if in-house programs are developed, however the time required conducting training means a loss of productivity in other areas.

Access control to the building is easy to implement with commercial off the shelf (COTS) products such as smart cards with photographs and finger scans. This single measure combined with door lock scanners meets most of the security requirement for the Company. By linking into the existing Oracle database, there is a lower barrier to implementation since personal data can be centrally stored for uses ranging from HR to access controls to grades.

Perhaps the most difficult cost to analyze is the effect of limited access based on job description, department, and need to know. The hours necessary to adequately describe department access requirements must be combined with a certain loss in productivity that comes from preventing users having complete network access at all terminals. As an example, compartmentalized information must only be accessed in secured spaces cleared for this information. The costs associated with providing physically secure, and electronically secure rooms are significant. However, the initial investment in secure rooms mitigates the long-term vulnerability of less stringently controlled access in which information may inadvertently be overseen. Therefore, risk is reduced.

Finally, the manpower required to ensure an adequate physical security presence adds to HR costs especially since these personnel must also posses security clearances for the spaces to be monitored. This means no minimum wage employees!

3. Internet Border Protection

Reasons for concern – The first layer of any network defense usually lays at the connection between corporate assets and the external network – in this case the Internet. A defense in depth strategy described in SANS 9.1 coursework requires several integrated systems functioning in concert together to provide multiple protections from various threats. The next logical layer of protection after the physical building is the logical controls limiting access into the electronic network. GIAC's need to access the Internet for personal and business use exposes corporate assets to potential attack or theft and therefore limited access both into and out of the network is required.

Perceived Threats and Consequences – Any system exposed to the Internet or other means of user inputs poses a threat to network security. The only sure means of security is to never turn the machines on – but this is not a practical solution.

Hardware and software are both vulnerable to hacking or misuse both from external and internal sources. As previously addressed, half of this equation is handled through limiting access to hardware to only those persons with the proper job description. This mitigates malicious physical attack as well as limiting the exposure to internal hacking since computers that are the most vulnerable to internal hackers have limited access controls and layered physical and logical monitoring.

External hacking is considered a significant concern since the preponderance of software on the GIAC network is Microsoft based. The overall threat to network security is raised – not so much because of inherent MS vulnerabilities, but because MS systems are a favorite target for malware/spyware attacks.

The consequences of introducing malicious code in the form of viruses, Trojans, worms, or back doors include lost or stolen data, compromised exam and lesson plan security, and ultimately loss of accreditation.

Mitigation – Several steps are necessary in developing a defense in depth strategy to protect assets from misuse or misappropriation. This area only addresses logical access to the firewall, routers, and switches to guard against hacking attempts.

The first layer lies at the firewall including its proper installation and configuration to provide proper port blocking and/or packet filtering to ensure adequate security while still providing ease of unclassified network access. In addition, an IDS is necessary to monitor the effectiveness of firewall functionality and configuration.

Inside the DMZ, access to resources such as study-guides and training materials is controlled using container and user access control lists. In addition, by filtering IP addresses and subnets, traffic into or out of a network segment can be controlled in combination with the types of data stored in that segment. By limiting the programs available to users based on their need for access the number of sources of attack can be removed. User activity must be monitored through event logs, proxy logs, packet dumps, and resource monitoring policies.

The judicious application of rule sets and filters at the routers aids in detecting attempted hacking or other network attacks such as port scanning, DDOS attacks, or spoofing. Following vendor recommendations for hardware installation and configuration along with local guidance from prime contractors provides layered restrictions on network traffic.

Automated alerts associated with the IDS systems are necessary to provide real-time alerts to potential penetration or malware activity. Proper application of virus scans with frequent updates aids in minimizing the potential for the adverse affects of malicious software introduced through e-mail or Internet access.

Finally, physical security monitoring devices in areas with high potential for misuse may include cameras, badge controlled access doors using biometrics and PKI, entry alarms, enclosure alarms, cipher locks, and two-person controls. As discussed above, limiting physical access to key resources reduces the likelihood of hacking.

Implementation Costs – Good network hardware is expensive to purchase, maintain, and replace. In addition, to properly manage and configure this switching gear requires well-trained technicians; therefore, budget planning needs to include adequate phased replacement as well as a continuing training program to ensure current knowledge of events. As example, the recent publication of SNMP weaknesses requires reconfiguring of all the Cisco devices in the network.

Additional costs are associated with the purchase and licensing of IDS software and with adequate training of analysis personnel. Network security and information systems officers require training and tools necessary to create, monitor and interpret network traffic. As example, the GISO course was deemed necessary for GIAC's ISSO in an effort to broaden experience and gain insight into current events.

The greatest potential cost, however, could be loss of access to the database or theft through data mining techniques; therefore, exceptional protection of the central database is critical to the success of this method. To support database integrity, separate backup systems and log monitoring is required as well as several DBAs to maintain the system.

4. Logical Access Controls

Reasons for concern – Nearly all research points to one undeniable statistic that internal threats outweigh external for one primary reason – ease of access. People fail, and it is the human failure that most security systems are least prepared to handle. From the inside, an employee with elevated access privileges can move or destroy data while bypassing trip wires designed to prevent the same manner of outside activity. Since GIAC houses proprietary information critical to mission success, it is vital to heighten individual awareness toward appropriate use policies. This section specifically addresses the proper implementation of NOS access controls to limit user access to information based on defined roles and job responsibilities.

Perceived Threats and Consequences – Firewalls, proxy services, and routers are all configured to examine inbound/outbound traffic for information matching specified rules sets. However, even detailed rules cannot prevent access if employees have inappropriate rights or permissions.

The most likely internal network threat comes from having inappropriately configured network access privileges or misrepresentation using someone else's logon. The physical network design coincides with the placement and storage of software and data based on its sensitivity. If GIAC employees were to have access to information not pertaining to their security clearance, or within their need-to-know, significant compromise of corporate assets could occur. As example, students with access to exam questions and answers would invalidate the training program. Additionally, staff members with access to network assets such as the servers, or having unlimited rights on their workstation could compromise system integrity.

The ability to hack the network from within poses a threat from disgruntled employees or from would-be computer experts trying to prove their skills. This compromise can occur if network access is not properly limited to that consistent with the job description

Mitigation – First and foremost, in any case dealing with people is the necessity for regularly scheduled security training. This means new user indoctrination briefs on acceptable use policies for the LAN/WAN and its resources. Additionally, quarterly training on rotating subjects relating to Company security should be required.

Establishing well-defined user roles and groups that have properly identified access rights is essential. In addition, periodic assessment of user rights and access limits must be part of a regularly scheduled audit. Following the requirements of the Orange book in meeting C2 integrity standards and access controls ensures uniqueness of user accounts and the monitoring and auditing of network access.

Protecting against elevated access privileges also requires the use of frequently changing passwords and enforcing complexity standards. Proper control of passwords and logins prevents account misuse or identity theft through misrepresentation on the network.

Access controls for critical hardware are limited to key personnel with divisions of labor playing a key role in preventing one person from having network wide access. This means that administration of firewalls and routers is separate from accounts, NOS, and software administration. It also means password protection of all configurable network assets and in some cases preventing remote network management to prevent hacking into configuration options.

In addition, to prevent the introduction of infected files by users, measures to disable input peripherals such as floppy drives and cd-roms are required. In this company, there are practically no end-users that actually "need" these devices (though many may disagree.) With the aforementioned upgrade to Win2K, the USB ports on computers must be disabled in BIOS or physically disconnected to prevent easy access to personal storage devices such

as thumb drives. Supporting this effort also requires minimizing driver loading to prevent auto detection of devices in a PNP environment. It also requires proper attention in the phased replacement of equipment to ensure PS2 devices (mice, keyboards, individual printers and scanners) rather than USB are purchased in sufficient quantities.

Since programs such as Gator or Comet cursor have built-in elevated privileges for installation, it is highly recommended that software inventories be taken on a regular basis (SMS is a great tool for this purpose.) Frequent network scans coupled with regular reminders of acceptable use will go a long way to preventing misuse.

Implementation Costs – Training of personnel is part of any good corporate model and is relatively inexpensive to conduct in-house. It can come in the form of interoffice memos, posted access to policies on the company Intranet, tips in management meetings, and streaming updates in classrooms as headers or trailers in a lesson plan. Regular exposure keeps security awareness at the forefront of daily activity.

As hardware shifts more toward USB being the only method of peripheral inputs, it will likely be necessary to purchase security enclosures for computers that prevent access to anything but the power/reset buttons. Many are already deployed in the classrooms at a cost of $200 per computer. The main drawback to this approach is that during phased replacement, if computer case designs change then the old enclosures must also be replaced.

The personnel costs associated with other implementations such as system wide software scans increases IS&T's workload as well as putting increased load on network resources. In addition, periodic assessments require in-house as well as contracted network audits that have personnel and service costs. The prime contractors take on part of this role in policy checking, and the ISSM/NSM are locally responsible for implementing the program.

5. Data Integrity and Storage

Reasons for concern – Since GIAC provides proprietary training to federal employees through privately developed software applications, it is critical to the company mission to maintain 100% accountability and access to this information. With over 12,000 students annually, the loss of even a few hours of teaching could cost tens of thousands of dollars. The focus of this section is on the backup and recovery of valid data to ensure business continuity.

Perceived Threats and Consequences – Several threats place GIAC at risk of not achieving its primary training and development goals. These can be categorized into manmade, natural disasters, and accidental.

The most difficult to protect against is manmade losses since these usually are the cause of deliberate sabotage or theft. Loss can come in the forms discussed above through hacking or virus activity either by denial of service, erasure, alteration, or removal.

Natural disasters prone to the geographic area where GIAC resides include tornadoes, hurricanes, fire, and infrequent earthquakes. The campus buildings are built to standards for these occurrences; however, fire inside the main building could cause significant loss of data.

Accidental loss is usually caused by careless work habits, or through the malfunction of equipment such as HHD, failed media, faulty media, backup machines, failed power supplies, failed UPS devices, malfunctioning RAID controllers, or motherboards. Data loss can be as simple as the accidental deletion of an important e-mail, or as serious as the corruption of exam data through alteration or physical failure of hardware.

Mitigation – The first measure of protection any network administrator will recommend is consistently good backups. The GIAC program includes a variation on incremental, differential, and full backups of all critical data throughout the week. A full backup occurs at least weekly, or more often on some systems when significant data changes warrant more immediate attention.

Once backups are successful, tapes are rotated to off-site storage to ensure that localized disasters will not prevent the timely recovery of information. Additionally, at least ninety days of data are be maintained. Weekly tapes are stored along with copies of software in a fireproof safe in a secured room with fire suppression.

Losses due to theft have been partially discussed in previous sections. Physical access to the GIAC facility automatically subjects people to search and seizure rules defined by the company security plan. Use of the network automatically subjects all personnel to monitoring of activities to minimize the chance of theft.

Finally, diagnostic software and regularly scheduled recoveries from data sets aid in the early detection of hardware problems. Spare equipment is maintained on hand so that no single device will be cause for a network outage. The only exception to this is cryptographic gear that may not be stored as ready service spares due to federal restrictions.

Implementation Costs – Compared with the cost of permanently losing data, all best efforts should be made to ensure accurate and complete system backups and safe storage. Backup equipment is relatively inexpensive and easy to maintain. Four separate backup devices are required with associated tapes.

Physical security is an integral part of the reaction force at GIAC and costs several thousand dollars quarterly to rotate personnel for continuing training. A partnering effort has been made with local state and federal agencies to reduce costs through joint exercises. This focuses primarily on theft prevention, and to a minor extent on preventing sabotage using closed circuit monitoring.

The phased replacement budget currently has all equipment being replaced on a four-year rotation. With over 500 workstations, 20 servers, associated switching gear, and multimedia presentation equipment, the annual phased replacement and incidental maintenance costs

exceed $400,000. Additional associated costs include manpower to support assembly, testing, and deployment of equipment.

A final word must be directed at ensuring all policies, practices, and standards are understood as living documents subject to change in the face of circumstance. No document should be considered comprehensive enough to cover all cases or incidents. In addition, addenda to company policy should be undertaken carefully to prevent bogging down functionality in legislation. However, when a clear need to modify regulations emerges, new policy should be established and approved by the local ISSO, ISSM, and DAA, with oversight by upper management.

Security Policies:

Purpose:

To briefly describe outlined policies concerning three of the areas covered above in risk analysis and threat assessment. It is in no way comprehensive, and will reference outside source documents for format and suggested content control (see List of References.)

The specific areas covered will include:

General Discussion:

GIAC Enterprises utilizes numerous technologies designed around the central purpose of providing multimedia-based education. Because of this, there are equally numerous vulnerabilities that must be governed by standard best practices to ensure network functionality and security. For this company, the central approach is to provide only that amount of access necessary to ensure employee productivity meets job requirements. While security through obscurity is not the intent, it is generally understood that implicit denial with explicit permission to perform functions and access data systems will be practiced. All persons accessing GIAC facilities, whether the main campus, the LRCs, contractor offices, or through electron data interchange, are subject to the imposed restrictions. Use of GIAC resources in any form constitutes consent to monitoring, and to personal search and seizure. No property of GIAC Enterprises may be altered, borrowed, manipulated, or otherwise adapted to personal, private, or enterprise use without explicit consent from management.

1. Encrypted Network Traffic Policy:

Purpose:

This policy is designed to establish guidelines for controlling the flow of data traffic between the classified networks and the encrypted network. In general, this traffic will occur when information is updated to or from the prime contractors, or when secured telecommunications are required for conferencing.

Scope:

This policy applies to all GIAC employees and contractors while using data, or while involved in network transfers associated with the encrypted communications network of GIAC. It is intended to govern all systems located on the GIAC campus involved in encrypted communications traffic including all hardware and systems software physically and logically linked.

Policy Outline:

1. No data transfers shall occur without the express consent of the cognizant department director and the ISSM.
2. All data transfers shall occur during normal business hours.
3. All data transfers shall occur under the direct supervision of the ComSec officer, custodian, or ISSO, and shall incorporate two-person controls at all times.
4. A single storage point shall be established on the encryption server for receiving and preparing data for transfer/transmission both inbound and outbound.
5. A single storage point shall be established on each of the Proxy servers hosting the classified segment and multimedia development segments for receiving and preparing data for transfer/transmission both inbound and outbound.
6. Prior to any encrypted transfers, a secured line telephone connection will be established between the source and destination members to ensure proper controls at each end of the transfer.
7. All connections to the encrypted network shall be clearly labeled and marked in red including wiring, port identifiers, and each end of any associated cable runs.
8. Under no circumstances shall any encryption equipment be connected to an unsecured system.
9. All passwords and encryption keys shall be stored in the ComSec safe located in the server vault.
10. All actions associated with the encrypted network require two-person controls for validity and integrity assurance.
11. All data transfers shall follow a standard procedural check sheet to ensure complete and accurate transfers.
12. ComSec officers, custodians, and all information security staff shall have quarterly refresher training on procedures and regulations governing the handling of classified and encrypted material.

Responsibilities:

The DAA is ultimately responsible for compliance with corporate policies and may designate in writing an ISSM, ISSO, NSM, ComSec Officer, and ComSec Custodian with delegated authority for handling information security and assurance.

The ISSM shall approve all transfers of data to and from the encrypted traffic server, and in his absence this approval may be given by the ISSO. Exercise of this option shall be reported to the ISSM and DAA at the earliest possible opportunity. The ISSM shall schedule continuing training topics and periodic examination of ComSec/InfoSec personnel to verify adequate knowledge of procedures and policies. The ISSM shall make a regular report to the DAA of all data transfers at weekly senior staff meetings.

The ISSO will act as a secondary officer in the place of the ISSM when necessary due to unavoidable absence. The ISSO shall examine the methods of data transfer and ensure that designated data stores have been swept of residual data following the completion of each transfer process.

The ComSec officer and custodian shall have primary responsibility over the direct supervision of data transfers, coordination of messages, key coding and rotation, and shall report all activities to the ISSO and ISSM. They shall jointly make record entries in a log maintained in the ComSec safe for all data transferred to include date, time, content of material, keys used, and size of transfer. All equipment maintenance associated with encryption equipment is the sole responsibility of the ComSec officer and custodian.

All GIAC employees are responsible for the proper handling of classified or encrypted information and shall report abnormalities to the ISSO/ISSM immediately. Department directors are responsible for proper notification of the need to transfer data between the designated stores. Under normal operation, a 24-hour notice is required to ensure proper coordination of involved parties.

Penalties for Noncompliance:

All secured transmissions are controlled by Federal and DOD regulations and shall be controlled in accordance with governing documents. Failure to comply with regulations or to report mishaps could result in prosecution, termination of employment, federal criminal and punitive fines, and potential imprisonment.

Failure to follow locally generated policies or procedures could be deemed grounds for censure, fines, termination of employment, or prosecution depending upon the severity and nature of the violation. Personal integrity is vital to the handling of encryption equipment and transmissions; therefore, all employees should report even minor errors.

2. Logical Access Controls Policy:

Purpose:

This policy is designed to provide guidance for controlling network access through the proper application of the NOS. It also addresses the need to properly train all employees on basic network use and security issues.

Scope:

This policy applies to all GIAC employees, contractors, and authorized agents in the use of GIAC information and network resources. It is intended to govern the basic logical access controls measures for users of GIAC computers, intellectual property, and fundamental communications within the organization. It briefly addresses external communications.

Policy Outline:

1. All users of GIAC computer and communications related systems will receive indoctrination training within two weeks of reporting to work. This training will include the basic nature of the NOS, the use of logon names and passwords, control of passwords, selection criteria for passwords, available applications on the network, use of network shared resources such as printers and drive space, private drive space, e-mail systems, the company intranet, the Internet, and acceptable use policies.
2. All employees will receive quarterly training on rotating subjects relating to network use, security bulletins, and current events. These may come in the form of intranet postings, required reading articles, short presentations, or briefings at department or division meetings.
3. The general policy for all personnel employed by, or working in contract with GIAC Enterprises, is to restrict access to only information or applications necessary to perform normal work related functions within the individual's job description. This also requires the separation of duties to minimize the concentration of access rights and privileges. On a case basis, specific individuals may be granted additional rights, privileges, or access outside of their category and will be so designated in writing. This process will be specific in nature, proposed by the appropriate department supervisor, reviewed by the ISSO and NSM, recommended by the ISSM, and approved by the CIO with the concurrence of the DAA. Basic categories are described below and are subject to change as required.

   Category-1: Identifies all basic network users including students, physical security personnel, general administrative staff, and supervisors of a non-technical nature.

   Access Rights: Shall be limited to access of information and applications specific to their workgroup responsibilities and may include (but not limited to) the MS Office suite of applications, personnel management tools, financial suites, Internet and Intranet applications, and access to general public shared information. Each workgroup and department will have its own network storage space for public domain within the group. Each individual will have semi-private network storage for

personal use. All personal drive space on the network is subject to periodic monitoring for proper use and shall not contain material of an inappropriate nature as described in the acceptable use policy.

Category-2: Identifies all senior supervisory staff including upper management, executives, the CEO, COO, CFO, and department directors.

Access Rights: Shall be limited consistent with Category-1 above, and will include access to sensitive corporate information as required by job position and title. All additional access to applications and information shall be on a *need to know* basis consistent with best practices to ensure proper compartmentalization of corporate assets. A decision to elevate privileges in this category requires recommendation by the DAA, and consent by simple majority among category members. Elevation of executive rights should be exercised sparingly and only for specifically identified issues with a predefined time limit to prevent a loss of sensitivity to the least privileges policy.

Category-3: Identifies academic instructors, supervisors, and students.

Access Rights: Shall be limited consistent with Category-1 above, and will include access to the applicable portions of the academic network and its resources. All staff in this category will have the necessary privileges and rights to access materials within their specialty for the purposes of presenting, teaching, administering exams, tracking student progress, and other academic related activities. Students shall have similar rights, but be limited to the LRC network for all computer access. Under no circumstances shall any student be given access to any resources outside of the LRCs.

Category-4: Identifies all multimedia developers, local contractor representatives associated with development, and personnel responsible for communications with the prime contractors.

Access Rights: Shall be consistent with Category-1 and –3 above as appropriate. Personnel in this category shall have only that access necessary to administer the presentation and updating of academic multimedia materials on the LRC and academic portions of the greater network. Access to software applications and resources within the development network will be consistent with the particular work assignments and are fluid with the changing of team assignments. This means an individual may have elevated supervisory rights for a specific team project and will subsequently have their privileges demoted at the completion of that project. This is consistent with the movement of personnel into and out of development teams based on expertise.

Category-5: Identifies all IS&T hardware technicians.

Access Rights: Shall be consistent with Category-1 above, and shall include limited administrative rights within all networks necessary to affect local repairs to all

manner of network resources with the exception of security devices, routers, switches, or domain controllers. Personnel in this category shall have full network privileges on the test network for the express purposes of training and to enhance personal skills in applications, protocols, and practices required in providing network operational continuity.

Category-6: Identifies all IS&T administrators and hardware administrators not included in Category-5.

Access Rights: Shall be consistent with Category-1 and –5 above, and shall include rights to effectively manage all segments of the various networks at GIAC Enterprises. This includes all hardware and software within the confines of the campus, as well as coordination of all network traffic inside and outside of the networks. The appropriate divisions of labor will include a Senior Network administrator (SNA,) two assistants (ASNA,) and at least two hardware administrators (HA) responsible for routers, switches, firewalls, and domain controller support. The crypto equipment and Novell management will be handled separately by a Communications Security officer (CSO) and at least one assistant (ACSO.) Under no circumstances will communications security be treated as a collateral assignment of another network administrator. Additionally, two person controls on all communications security related issues will be strictly enforced including all equipment handling, administration, and transmissions. This mandate ensures non-repudiation in cryptographic transmissions and protects all associated personnel.

Category-7: Identifies all information security (InfoSec) personnel not previously discussed including, but not limited to, the NSM, ISSO, ISSM, SAT, CIO, and DAA.

Access Rights: Shall be consistent with Category-1, -5, and –6 above as appropriate, and shall include rights to effectively conduct security inspections and audits as deemed necessary by the DAA. Administrative network privileges will be exercised sparingly in accordance with best practice efforts to ensure non-repudiation within the organization. Elevated privileges will be authorized only for forensic purposes, and audit trails of all persons, entities, and applications will be exercised at all times. Only under specific instances of suspected corporate espionage or the loss of control of classified material will "stealth" auditing be authorized. In these rare cases, specific limited authority will be granted by the DAA under advisement of senior management in writing. It is unlikely that in-house agents will conduct forensic work, but rather that an external CERT will be sought independently; however, this provision is made for contingency planning purposes.

4. With the exception of SNA/ASNA and InfoSec personnel, no one shall have access to command prompts or other native NT4 tools that would allow network access outside of their predefined login rights. Development of personal tools, scripts, batch files, or utilities is expressly forbidden and every measure to prevent their development shall be made. Only designated programmers shall have access to software with the

purpose of developing applications, their front-end interfaces, or any multimedia extensions.

5. Orange book requirements will be used to define C2 requirements for NOS use and installation. The requisite NOS security policy files are provided by a key contractor, shall be examined, and installed by IS&T personnel.
6. Passwords shall meet complexity requirements to include a minimum of eight characters in length, and three of the following:
    a. Upper case letters
    b. Lower case letters
    c. Numbers
    d. Allowed special characters (specific to the NOS)
7. Passwords shall expire at ninety day intervals; up to 10 shall be remembered by the NOS; minimum password age shall prevent repetitive replacement in order to circumvent change requirements; account lockouts and release procedures shall be defined in more detail.
8. All computers, programmable switches, routers, firewalls, and encryption equipment shall have unique passwords assigned to their BIOS interface, and any login interfaces. Passwords shall meet complexity and age requirements.
9. Physical access to network devices in 8 above shall be limited to persons with appropriate job descriptions (e.g., SNA shall have access to servers, etc. . .)
10. Peripheral devices shall be disabled to the extent necessary to prevent the introduction of user software or utilities. This includes disabling floppy drives and CD-Rom drives in BIOS.
11. When the Windows 2000 operating system is introduced, all equipment with externally exposed USB ports will require security enclosures to prevent user access. This measure prevents the misuse of self-configuring devices such as thumb drives.
12. An acceptable use policy for Internet access shall be published outlining requirements for e-mail use, Internet use, and the necessity to prevent introduction of external software onto computers with access to the outside world.

Responsibilities:

All GIAC employees, contractors, and authorized agents are responsible for reading and adhering to company published policies. In addition, it is the individual's responsibility to attend continuing training and to be proactive in the enforcement of acceptable use practices.

The ISSM shall schedule all continuing training topics and shall appoint lecturers and methods for delivering the material as appropriate to the topic.

The ISSO shall conduct periodic checks information security policies to ensure compliance with currently posted requirements. This means identifying the proper revisions and updates to security policy files, applying necessary patches or hot fixes in light of posted security updates (such as the SNMP vulnerability,) an for ensuring network administrators are active in managing account creations and deletions for the company. The ISSO shall also review all audit logs for proper network activity.

The SNA shall direct user account management and ensure timely creation/deletion of users based on reports from HR. This is an important issue since student turnover is significant. User lockouts shall be directed to the ISSO for investigation prior to resetting passwords.

Management of network hardware will be the responsibility of the NSM with assistance from the SNA. Reports shall be made to the ISSO/ISSM upon completion of password changes, configuration changes, and any noted network abnormalities.

Penalties for Noncompliance:

All employees have the express responsibility to guard their accounts, passwords, and intellectual property in accordance with corporate and DOD security policies. Failure to adequately guard against the compromise of account security will be investigated by the ISSO/ISSM with oversight by HR to determine the nature of the infraction. Deliberate negligence is grounds for termination of employment, fines, and prosecution as directed by law.

Failure to attend training is a minor infraction, but shows poor character and sense of responsibility. All employees are strongly encouraged to follow training requirements.

Under no circumstances shall any employee, contractor, or authorized agent allow another to use their accounts. All actions taken under an account shall be credited to the account owner unless overwhelming evidence proves otherwise. (If you don't have the requisite access rights, direct a request to your supervisor for consideration of elevating access based on the need. If you "just want to check something" after you log out, don't compromise your neighbor by asking to use their account.)

Shoulder surfing is a serious violation of network security. Do not share your passwords, and do not attempt to learn someone else's. Violations of network security can lead to loss of security clearances, censure, termination of employment, fines, or prosecution as directed by law.

3. Backup and Recovery Policy

(Derived from Information Security Research Center Policy guide – See references section)

Purpose:

This policy is designed to provide guidance for controlling network data backup and recovery. It addresses the need to properly establish a baseline for software and data warehousing supported by regular backups with secure storage.

Scope:

This policy applies to all GIAC software and data used within the confines of the GIAC enterprise. A properly defined program ensures the reliable warehousing and recoverability of GIAC's electronic media to ensure business continuity. All servers and network attached storage (NAS) shall be included in this policy for regularly scheduled backups. In addition, key workstations with unique configurations shall be imaged for ready restoration. These computers will be included in the backup schema to ensure development changes made on local HDD are adequately covered. In the event of a HDD failure where a client has declined backup services, IS&T will only be responsible for reinstalling the standard client configuration defined in the IS&T Standard Operating Procedures manual.

Note: this policy specifically does not address losses caused by physical theft, removal, or natural disasters. These issues are addressed in the physical security manual and disaster recovery plan respectively.

Policy Outline:

1. A standard installation image for each type of workstation shall be made for the quick and easy restoration of computers in the event of a unit failure.
2. All unique installations shall be imaged upon completion of their build process for the quick and easy restoration of computers in the event of a unit failure.
3. All servers shall be image upon completion of initial configuration, and re-imaged following any significant changes in software arrangements.
4. All network devices (defined as servers, CD image servers, or NAS,) and unique workstations (defined as developer or programmer computers) shall be included in the following backup scheme:
    a. Monday – Full backup after normal working hours are completed,
    b. Tuesday-Thursday – Differential backup after normal working hours are completed,
    c. Friday – Full backup after normal working hours are completed,
    d. Saturday-Sunday – Incremental backup after normal working hours are completed,
    e. Daily – database backups using Oracle backup agent to NAS and designated storage on the BDC for redundancy.

5. Tapes shall be rotated in sets as defined in step-4 above, with weekly sets stored in the fire safe. On a monthly basis, tapes shall be rotated from the safe to an off-site storage unit.
6. A minimum of three month's backups shall be maintained off-site.
7. Once a quarter, sample sets of data shall be restored from tape to verify data integrity and IS&T's ability to recover information.
8. The maximum permissible downtime due to data loss should comply with the following scheme:
    a. Application software – 1 working day (WD)
    b. Server application software – 1 WD
    c. Workstation applications (critical) – 1 WD
    d. Workstation applications (non-critical) – 5 WD
    e. Oracle database information (critical) – 2 hours
    f. Oracle database information (non-critical) – 1WD
    g. Lessons or teaching presentations for the current day – 15 minutes
    h. Lessons or teaching presentations for other days – 1 WD
    i. Personal data or e-mail (critical) – 1 WD
    j. Personal data or e-mail (non-critical) – 5 WD
9. Regular IS&T training shall occur on data backup and recovery methods to coincide with the quarterly recovery tests.
10. Data redundancy shall follow the following basic scheme:
    a. Raid-0 on all server OS drives (two OS drives per server)
    b. Raid-5 on all server data stores

Responsibilities:

The SNA shall direct network administrative staff and technicians in the daily operation of server resources and shall report the status of backups to the ISSO. The SNA shall be responsible for monitoring the physical and logical condition of network storage devices and any associated maintenance.

Weekly data backup sets shall be given to the ISSO for storage in the fire safe. Rotation of tapes from the fire safe to offsite storage will be coordinated by the ISSO with transport duties assigned to the weekly IS&T technician on call.

The Oracle DBA is responsible for ensuring daily data backups are conducted and for the periodic verification of database backups. The Oracle DBA shall coordinate with the SNA for situational cold backups when major changes warrant.

It is the responsibility of all GIAC employees to adequately notify IS&T of the need for backing up data from other-than-normal data stores. In the event of lost data or improperly functioning software, a service request should be submitted from the company intranet specifying the nature of trouble and relative importance of the request.

The Help Desk supervisor will assign a final priority and forward the request to networking personnel for review and disposition. Upon completion of data restoration, the

Help Desk is responsible for following up with a courtesy call to assess the adequacy of customer support.

Penalties for Noncompliance:

The ultimate consequence associated with failing to execute a proper data assurance program is permanent loss of information. This could lead to company discredit, failure to properly safeguard privacy act information, or the inability to achieve the company's primary goal of training.

Any inability to restore lost or corrupted data within the policy guidelines should be directed to the respective supervisor for remediation. The SNA or ISSO as appropriate should make every effort to ensure that customer service meets the published timelines.

Failure to carry out the normal daily routines as delineated in the IS&T standard operating procedures manual pertaining to backups and restoration of data could result in censure, reprimand, fines, or termination of employment if warranted.

Theft of company information is dealt with in the physical security manual and shall be handled by HR, Legal, the ISSM, and NSM.

These general policies are subject to change with developments in network architecture, both logical and physical, and as new security-analysis results are presented by higher authority. The ISSM will forward all proposed changes through the CIO to the DAA for final approval. Revisions should be posted to the corporate Intranet when widest distribution is required.

Assignment-3: Defined Security Procedures

Methods for Transferring Data between the Various Network Segment

General Discussion:

This section gives guidance on the transfer of material between the network segments and the basic control of InfoSec between the levels of classification. This guidance is not intended to cover every possible situation; therefore, if there exists doubt in the mind of anyone involved in data transfers, contact the ComSec Officer or ISSM for clarification.

There are four basic types of possible data transfers: 1) from the Encrypted segment to the Classified segment, 2) from the Classified segment to the Encrypted segment, 3) from the Classified segment to the Unclassified segment, and 4) from the Unclassified segment to the Classified segment. All data transfers shall be supervised regardless of the level of transfer; this meets the company's requirement for two-person controls governing InfoSec and ComSec handling.

1. Encrypted to Classified:

This type of transfer is used for bringing information into the organization from the prime contractors and requires the presence and direct supervision of either the ComSec Officer or the ComSec custodian. Two-person controls must be in effect at all times. All transfers will occur during normal working hours unless otherwise authorized in writing by the ISSM.

(DT≡Duty Technician, CSO≡ComSec Officer, CSC≡ComSec Custodian)

a. The ISSO will notify the DT and CSO/CSC when a transfer is required, including date and time.
b. The ISSO will obtain permission from the ISSM to make a data transfer and will make a journal entry in his general transfer log (GTL) when the transfer is complete including date, time, type of data transfer, size of transfer, and personnel involved.
c. The CSO and DT will secure the server vault by locking the door with both locks, and will post a sign outside the door forbidding entry until further notice.
d. The CSO will contact the transmitting organization and make the necessary arrangements for data transfer.
e. The DT will obtain the encrypted transfer log (ETL) from the safe, and the data transfer checklist from the IS&T standard operating procedures manual.
f. The DT will verify that the data store directory is empty of any information. The CSO/CSC will verify.
g. Data transmission may now commence. Decryption occurs automatically.
h. The transferred files shall be scanned using corporate anti-virus software during the transfer process.

i. When all data is received, the DT and CSO/CSC will both acknowledge the file sizes and type, and will record this in the ETL. The CSO/CSC will verify with the sender that all data was transferred and then break connection.
j. Using a designated Transfer Agent account, the DT under CSO/CSC supervision will transfer the data to the designated data storage directory on the classified segment, and will remove all data in the encrypted store.
k. Once transfer is complete, the DT and CSO/CSC will sign and date for the transfer, and return the ETL to the crypto safe.
l. When all systems are restored to normal, the server vault may be unlocked and warning signs may be removed.
m. Completion of the transfer shall be made promptly to the ISSO and ISSM.
n. The ISSO shall verify that the old data store is empty and will contact the appropriate department director to transfer their data to the designated final working directory.
o. The data shall be scanned once more during transfer using corporate edition anti-virus software.
p. The ISSM will report to the CIO and DAA in a weekly report any and all transfers.
q. The check sheet used for the transfer shall be returned to the ISSO for filing.

All transfer logs and paperwork shall be maintained for three years in accordance with company retention policy. It is important for all personnel involved in data transfers to ensure proper procedural compliance to guarantee the validity of information security. Logs are maintained as objective quality evidence that proper controls were taken at each step and are designed to aid the operators. They act as a tool to protect against accusations of improper handling and should be adhered to strictly.

2. Classified to Encrypted:

This type of transfer is used for transferring information out of the organization to the prime contractors and requires the presence and direct supervision of either the ComSec Officer or the ComSec custodian. Two-person controls must be in effect at all times. All transfers will occur during normal working hours unless otherwise authorized in writing by the ISSM.

(DT≡Duty Technician, CSO≡ComSec Officer, CSC≡ComSec Custodian)

a. This procedure duplicates many of the steps outlined above and will be abbreviated as a reversal of procedure-1. This includes the transfer of data from the multimedia developmental segment to the prime contractors for review.
b. The ISSO will notify the DT and CSO/CSC when a transfer is required, including date and time.
c. The ISSO will obtain permission from the ISSM to make a data transfer and will make a journal entry in his general transfer log (GTL) when the transfer is complete including date, time, type of data transfer, size of transfer, and personnel involved.
d. The ISSO will ensure the necessary data is transferred from the respective department data storage to the classified network transfer storage directory.

e. The CSO and DT will secure the server vault by locking the door with both locks, and will post a sign outside the door forbidding entry until further notice.
f. The CSO will contact the receiving organization and make the necessary arrangements for data transfer.
g. The DT will obtain the encrypted transfer log (ETL) from the safe, and the data transfer checklist from the IS&T standard operating procedures manual.
h. The DT will verify that the data store directory is empty of any information. The CSO/CSC will verify.
i. Using a designated Transfer Agent account, the DT under CSO/CSC supervision will transfer the data from the designated classified data storage directory to the encrypted data storage, and will remove all data from the classified store.
j. The data shall be scanned during transfer using corporate edition anti-virus software.
k. Data transmission may now commence. Encryption occurs automatically.
l. The data shall be scanned again outbound with corporate edition anti-virus software.
m. When all data is sent, the DT and CSO/CSC will both acknowledge the file sizes and type, and will record this in the ETL. The CSO/CSC will verify with the receiver that all data was received and then break connection.
n. The DT will remove all data from the encrypted data store.
o. Once the transfer is completed, the DT and CSO/CSC will sign and date for the transfer, and return the ETL to the crypto safe.
p. When all systems are restored to normal, the server vault may be unlocked and warning signs may be removed.
q. Completion of the transfer shall be made promptly to the ISSO and ISSM.
r. The ISSO shall verify that the old data store is empty.
s. The ISSM will report to the CIO and DAA in a weekly report any and all transfers.
t. The check sheet used for the transfer shall be returned to the ISSO for filing.

3. Classified to Unclassified:

This type of transfer is used for transferring information from the classified segment of the network to the unclassified network. Primarily, these transfers occur in support of the LRC curriculum when program updates are required. As with others, these transfers require the presence and direct supervision of either the ComSec Officer or the ComSec custodian. Two-person controls must be in effect at all times. All transfers will occur during normal working hours unless otherwise authorized in writing by the ISSM.

It is important to understand that very few transfers of data occur from the classified network to the unclassified network. Some examples of instances follow:

a. Pushing updates to student study curriculum on the LRC,
b. Transferring information from the classified intranet to the unclassified intranet (e.g., policy statements, memorandums, etc.)

The only file types authorized for transfer from classified to unclassified networks are text (.txt), rich text (.rtf), hypertext (.html), ASCII comma delimited text, file interchange format graphics (JPG, JPEG), bitmap graphics (BMP), or graphical interchange format (GIF) since these file types do not contain hidden macros or complex compression of data.

(DT≡Duty Technician, CSO≡ComSec Officer, CSC≡ComSec Custodian)

a. The respective department director will notify the ISSO that a need exists for transferring data to the unclassified segment.
b. The ISSO will notify the DT and CSO/CSC when a transfer is required, including date and time.
c. The ISSO will obtain permission from the ISSM to make a data transfer and will make a journal entry in his general transfer log (GTL) when the transfer is complete including date, time, type of data transfer, size of transfer, and personnel involved.
d. The ISSO will ensure the necessary data is transferred from the respective department data storage to the classified network transfer storage directory.
e. The DT will run a company "dirty word" search program looking for key proprietary information on all files to be transferred. The CSO will verify the scan is complete and that the files are clean prior to authorizing transfer.
f. The files will be scanned with corporate anti-virus software.
g. Using a designated Transfer Agent account, the DT under CSO/CSC supervision will transfer the data from the designated classified data storage directory to the unclassified data storage directory.
h. The data will again be scanned on the unclassified segment using corporate anti-virus software, and then transferred to the appropriate destination store.
i. The DT will remove all data from both the classified and unclassified data stores.
j. Completion of the transfer will be reported to the ISSO who will verify that the transfer data stores are empty.
k. Only study curriculum changes will be reported to the ISSM for inclusion in the weekly letter.
l. The check sheet used for the transfer shall be returned to the ISSO for filing.

4. Unclassified to Classified:

This type of transfer is used for transferring information from the unclassified segment of the network to the classified network. Primarily, these transfers occur in support of the administrative and development staff. In an effort to minimize the generation of classified material, most work is performed on the unclassified network segment with transfers of administrative material to the classified network when repetition is required. Additionally, some material such as software updates, hot fixes, virus definitions, and the movement into the more secured networks of mail attachments requires their transfer (e.g., all attachments are stripped from e-mail inbound to the classified network for virus and malware scans.) As with others, these transfers require the presence and direct supervision of either the ComSec Officer or the ComSec custodian. Two-person controls must be in effect at all times. All transfers will occur during normal working hours unless otherwise authorized in writing by the ISSM.

(DT≡Duty Technician, CSO≡ComSec Officer, CSC≡ComSec Custodian)

a. The respective department director will notify the ISSO that a need exists for transferring data to the classified segment.
b. The ISSO will notify the DT and CSO/CSC when a transfer is required, including date and time.
c. The ISSO will obtain permission from the ISSM to make a data transfer and will make a journal entry in his general transfer log (GTL) when the transfer is complete including date, time, type of data transfer, size of transfer, and personnel involved.
d. The ISSO will ensure the necessary data is transferred from the respective department data storage to the unclassified network transfer storage directory.
e. The files will be scanned with corporate anti-virus software.
f. Using a designated Transfer Agent account, the DT under CSO/CSC supervision will transfer the data from the designated unclassified data storage directory to the classified data storage directory.
g. The data will again be scanned on the classified segment using corporate anti-virus software, and then transferred to the appropriate destination store.
h. The DT will remove all data from both the classified and unclassified data stores.
i. Completion of the transfer will be reported to the ISSO who will verify that the transfer data stores are empty.
j. The check sheet used for the transfer shall be returned to the ISSO for filing.

Summary:
These procedures for data transfer are aids to the operator and are intended to be used in combination with the signature check lists provided in the IS&T standard operating procedures manual. Any changes must be requested through the ISSM. A copy of these procedures should be posted on the corporate intranets in the IS&T references section.

List of References

Fried, Stephen. "9.1 SANS Security Leadership," part 1.1-8.

Information Security Research Center. Chapter 3.4 " Data Backup Policy."
URL: http://www.isrc.qut.edu.au/bsi/b/34.htm

McCullagh, Adrian, and William Caelli. "Non-Repudiation in the Digital Environment." 19 July 2000.
URL: http://www.firstmonday.dk/issues/issue5_8/mccullagh/

Bartlett, Terry. "Information Assurance Readiness Assessment." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000.
URL: http://csrc.nist.gov/csspab/june13-15/Bartlett.pdf

NSWC Dahlgren Computer Security Incident Handling Procedure, October 1996.

Holbrook, P. and J. Reynolds, Ed. "RFC1244, Site Security Handbook." July 1991.
URL: http://www.faqs.org/rfcs/rfc1244.html

Fraser, B., Ed. "RFC2196, Site Security Handbook." September 1997.
URL: http://www.faqs.org/rfcs/rfc2196.html

Fraser, B., Ed. "FYI/FYI8, Site Security Handbook." September 1997.
URL: http://www.faqs.org/rfcs/fyi/fyi8.html

Sun Microsystems, author unknown. "How to Develop a Network Security Policy: An Overview of Internetworking Site Security."
URL: http://www.sun.com/software/white-papers/wp-security-devsecpolicy/

Internet Security Systems, author unknown. "Penetration Tests: The Baseline For Effective Information Protection." A white paper. URL: http://www.iss.net/

SANS READING RESOURCES (GISO Section)

Nichols, Arthur. "A Perspective on Threats in the Risk Analysis Process." 31 August 2001.

Hazel, Lorraina. "An Overview of Oracle Database Security Features." 13 May 2001.

Mina, Ted. "Application Security, Information Assurance's Forgotten Stepchild – A Blueprint for Risk Analysis." 26 July 2001.

Orey, Douglas T. "Free NT Security Tools." 6 August 2001.

Swartz, Bruce. "Information System Security Evaluation Team: Security Insurance?" 27 July 2001.

Krupa, Andy. "The Oversight of Physical Security and Contingency Planning." 21 August 2001.

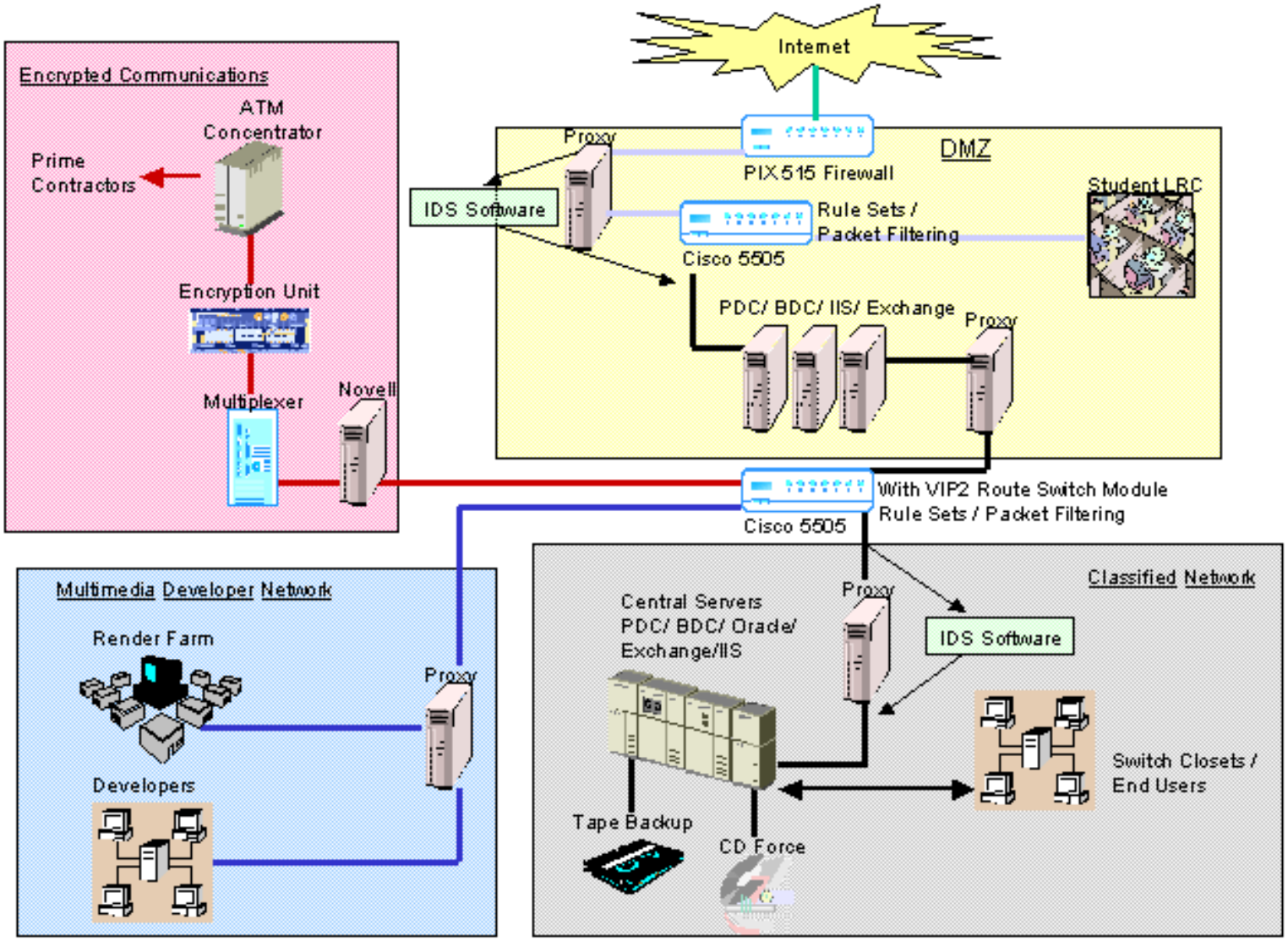
Nichols, Peter. "Vulnerability Scanning in the Corporate Enterprise." 21 June 2001.

Additional Government References:

Procedural references, format, and examples were derived from the following specific documents along with guidance from the current security manager.

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No.4009, National Information Systems Security Glossary, August 1997.
2. NTISSD 500, Information Systems Security (INFOSEC) Education, Training, and Awareness, 25 February 1993.
3. NTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, 16 November 1992.
4. NTISSD 502, National Security Telecommunications and Automated Information Systems Security, 5 February 1993.
5. DOD 5200.40, DOD Security Certification and Accreditation Process (DITSCAP)
6. IA Publication 5239-01, Introduction to Information Systems Security.
7. IA Publication 5239-04, Information Systems Security Manager Guidebook.
8. IA Publication 5239-07, Information Systems Security Officer's Guidebook.
9. IA Publication 5239-08, Network Security Officer's Guidebook.
10. IA Publication 5239-11, System Security Requirements.

Appendix-A: NETWORK DIAGRAM



Appendix-B: HOT FIX / PATCH ORDER SCHEDULE

	Service Patch / Hot Fix / Action	* Q299444, Q301625 do not self install with MS update services and will have to be applied from the central updates storage directory on the file server. # http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp
1.	NT 4.0 Service Pack 4.0	
2.	IE 4.01 with Active Desktop	
3.	NT 4.0 Service Pack 6.0 128-bit Encryption	
4.	IE 6.0	
5.	NT 4.0 Service Pack 6.0a	
6.	NT 4.0 Post SP 6.0a Roll Up	
7.	Apply updates from http://windowsupdate.microsoft.com	
8.	Run Hfnetchk with the switches (-b –v)	
9.	Apply MS01-041, Q299444 (*)	
10.	Apply MS01-044, Q301625 (*)	
11.	Ensure review of Technet for further updates (#)	
12.		
13.		
14.		
15.		