Global Information Assurance Certification Paper

GISO Basic Practical Assignment

Version 1.2

Kandi Dillard

Assignment 1 - Description of GIAC Enterprise and the nature of its business

Overview of GIAC Enterprise

GIAC Enterprise is a subsidiary of a larger non-profit research organization whose broad range mission is to promote public health and research health concerns that plague mankind. Located at a remote facility, GIAC Enterprise has a more refined mission, which is to study the causes of cancer and to develop new methods for its detection and treatment. Researchers at GIAC Enterprise study a wide range of factors such as the biology of cancerous tissues, genetic predispositions of cancer patients and the environmental factors that lead to forms of the disease. The long-term goal of GIAC is to achieve a better understanding of this disease so it may detect and treat as well as someday prevent or cure it.

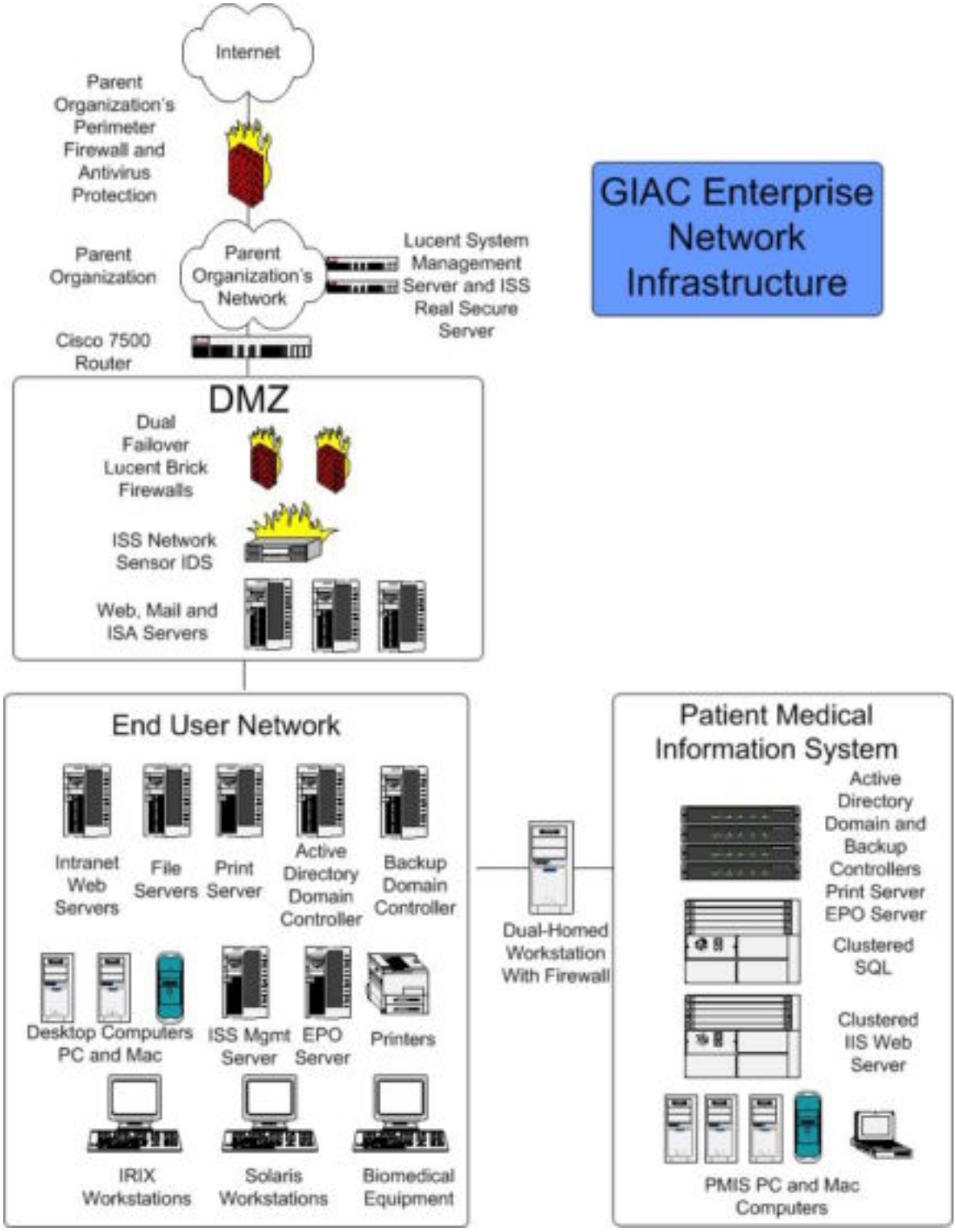
The location of GIAC's parent is not conducive to a large number of individuals who have various forms of cancer. Because of this, GIAC is in a different geographic region than its parent company. As such, GIAC operates its own treatment/outpatient facility as well as a 16-bed inpatient wing where participants may stay and be studied and/or treated for prolonged periods of time. Any treatment, diagnosis, medication or procedure performed on a study participant is a benefit of being part of the research study and therefore free of charge. Because GIAC does not perform testing of all biological specimens on site, any specimens sent to contracted laboratories get unique identification numbers that cannot be linked to participants by the labs. In addition to human participants, GIAC also has specialized controlled facilities under which animal studies are performed. Animal protocols are stringent in that all environmental factors such as lighting, food, temperature, humidity and bedding are closely monitored and controlled.

Considerably smaller than its parent organization of 11,000 employees, GIAC has on staff approximately 475 people of various levels of education and ethnicity. GIAC employs physicians, nurses, physician assistants, research and radiology technicians, administrative staff, facility workers, housekeepers, animal care givers, biologist, chemists, geneticists, researchers, plumbers, electricians and security staff to name a few. There are approximately 15 information technology staff members that support the GIAC mission. Because it is a research facility, which gets its operating funds from grants, the average researcher is employed for approximately two years. Unlike a hospital, the 16-bed inpatient ward and treatment/outpatient facility only treats and/or examines persons that have been admitted to a research protocol. Research protocols may be written to study malignancy traits, effects of new drugs on carcinoma growth or even develop better methods to target bad cells using radiation or

drugs. Similarly, blood and other biological samples taken from participants are analyzed to find better methods of treatment and diagnosis.

As a non-profit organization, GIAC is also involved in the dissemination of educational materials as well as publicizing its findings and advancements via its public websites. Among those who utilize GIAC's information are educators, students and researchers, as well as those who want to learn more about cancer and cancer treatments.

IT Infrastructure Overview



GIAC Parent Infrastructure

GIAC is connected to its parent company through a T3 connection. This leased line allows connectivity to GIAC's parent as well as to the Internet. The Cisco router that is maintained by GIAC's parent organization's IT department currently runs IOS version 12.0, including 23 software revisions. It also enables rules on the GIAC Cisco router to deter IP spoofing just prior to GIAC's firewall. GIAC only has control over the infrastructure *after* the Cisco 7500 router. Another service provided by the parent is a border firewall that has basic filtering rules such as HTTP and FTP filters enabled. All firewalls are managed using the centrally located Lucent Security Management Server (LSMS) at the parent's headquarters. The LSMS runs version 5.1.338 of both the LSMS server and Brick software that is updated by the IT department of the parent organization. GIAC's parent also scans all incoming and outgoing MS Exchange and SMTP email for viruses as well as running a perimeter intrusion detection system. GIAC's network consists of three major areas; the demilitarized zone (DMZ), the End User Network (EUN) and the Patient Medical Information System (PMIS).

Demilitarized Zone

The demilitarized zone is created using a failover pair of Lucent Brick 201 Firewalls (Brick) and an Internet Security Systems (ISS) Real Secure sensor for network-based intrusion detection. According to Lucent Technologies product literature at http://www.lucent.com/livelink/0900940380004b3b_Brochure_datasheet.pdf, if the active Brick in the failover pair fails, it will take approximately 400 milliseconds for the inactive Brick to resume protecting the network (3). The Brick is a hardened appliance with a proprietary operating system that will fit on a single floppy. The Brick can perform stateful packet inspection as well as monitor programs such as RealAudio using application level security. At GIAC, the Brick is used to filter packets to the DMZ. For example, the firewall will only allow port 443 connections to the Outlook Web Access web server so only incoming HTTPS connections from outside of GIAC are accepted. Similarly, connectivity to web servers might only allow HTTP and FTP requests from external sources such that educational materials may be downloaded or viewed. Since GIAC is responsible for its own infrastructure, the parent organization gives access to the LSMS allowed through 3 management consoles at GIAC that are locked down by user name, password and IP address. The ISS Real Secure network sensor, which is managed by the ISSO via a management console on the end user network, is placed directly after the firewall but prior to the devices in the DMZ to detect any intrusion from external sources as well as any suspicious activity leaving GIAC. The ISS network sensor runs on a hardened Windows 2000 server.

The DMZ itself contains externally accessible Microsoft Internet Information Servers and Macintosh web servers, a Microsoft Internet Security an Acceleration server and a Microsoft Exchange 5.5 email server. Web sites

house both FTP and HTTP services that allow public access to educational materials, employee access to secure web based email and researcher access to articles available in Portable Document Format (pdf) when they are away at conferences or out of the country giving lectures. Mail services need to be able to communicate only to the main email server at the parent organization and is locked down to the main email server for external connections. In order to access their email securely from anywhere, GIAC staff use Outlook Web Access that that runs on a stand-alone Microsoft Internet Information server. Microsoft's Internet Security and Acceleration (ISA) Server software product literature found at http://www.microsoft.com/isaserver/evaluation/productguide_v1.1.doc indicates that the ISA server can provide "filtering at the packet, circuit, and application layer, stateful inspection to examine data crossing the firewall" (1). GIAC utilizes the web proxy service to connect and protect the End User Network to the parent organization as well as to the Internet. In addition, the ISA server also secures incoming and outgoing traffic through stateful packet inspection as well as application layer filtering.

End User Network

The End User Network is the primary network used by approximately 400 end users for email, word processing, statistical analysis, non-patient data collection and other scientific applications and is comprised of a mixed platform of computers. For example, several Silicon Graphics computers have been implemented for chemical modeling and analysis. Another set of researchers utilize Sun Solaris workstations to analyze images from sources such as positron emission tomography. The remaining end user desktops are divided 70% running Windows 2000 and 30% running Macintosh OS 9.0. The majority of servers are of the Compaq Proliant series with a few Dell Power Edge servers. Servers generally have a single function so that in the event of a failure, multiple services are not affected. GIAC currently utilizes Windows NT technology for the Primary and Backup Domain Controllers. Windows 2000 servers are used for print services, intranet web sites using Internet Information Server 5.0, ePolicy Orchestrator 2.5 and Ripple Tech's LogCaster log file monitoring and alerting software. All servers at GIAC are attached to emergency power through uninterruptible power supplies so that during the transition, power is maintained. GIAC employees may house collected data and documents on workstations or on GIAC's file servers. As mentioned earlier, the End User Network contains a management console for the ISS Real Secure Network sensor that protects at the perimeter of GIAC's infrastructure.

Patient Medical Information System

The Patient Medical Information System is highly relied upon to provide access to patient charts. This network does not have Internet accessibility with the exception of a single dual-homed computer that is connected to the End User Network. This single computer retrieves encrypted patient lab results from a contracted lab's secure web site through a scheduled job that was created to

specifically authenticate and retrieve secure results for lab tests. The proxy server further locks this computer down so that it may only make a connection with a single IP address on the Internet. To further secure this computer and the highly sensitive network to which it is connected, Norton Personal Firewall 2002 is configured so that only connectivity to the web site of the contracted lab secure web site is allowed. This single computer has minimal services running as well as a special user account that has the ability to place reformatted data into a file on a share located on a server in the Patient Medical Information System network. The crown jewel of GIAC is the backend patient database that sits on a clustered Compaq server running Windows 2000 Advanced Server with SQL 2000. The cluster offers fault tolerance and redundancy since both clusters share the data located on a series of disks in a RAID 5 array. Access to the data on the server is based on SQL roles that authenticate the end user. Further data protection is added by a strict backup plan as well as replication to a failover server physically located in a different portion of the GIAC building under badge access in case of catastrophic incident. The PMIS network has a clustered web server that provides access to specific database information to medical professionals and researchers again based on SQL roles. The computers on this stand-alone network run Windows 2000 and have been locked down such that end users may only run a small Microsoft Access 2000 front end to access the backend patient database. This Window 2000 active directory network has its own domain controllers, printer server and McAfee's ePolicy Orchestrator v2.5 server. McAfee's ePO maintains policy and definitions for antivirus software reporting any infection detection.

GIAC Business Operations

Overview of business activities

As a non-profit research organization, GIAC employs a number of business functions to achieve its mission. For example, GIAC researchers and physicians utilize the Patient Medical Information System for treating, charting and collecting data from participants in research protocols. Being the crown jewel of GIAC, the patient data must be accessible at all times in case of medical emergency. In addition, GIAC must foster an atmosphere in which doctors, scientists, researchers and other staff may perform day to day tasks such as ordering supplies online, running experiments on biomedical equipment, collecting data, performing genomic research on national databases and collaborating with other scientists and doctors on the other side of the world. Finally, GIAC must provide the public with educational pamphlets and documents as well as recent GIAC press releases, discoveries and scientific publications on its web sites.

Applications and Access

In order to perform their daily activities employees require various types of access to complete their daily tasks. For example, all GIAC employees must have email for collaboration and correspondence with everyone from vendors to

universities. Employees on the End User Network must also have Internet access for tasks such as placing online orders for supplies, researching scientific information and communications with the parent organization's databases. In addition, they must be able to use network printers and be able to download and upload datasets and other information via file transfer protocol (FTP). To increase productivity, a number of fixed IP web sites are available on the intranet so that users in the same departments may collaborate and update their collected data from any workstation on the intranet. Similarly, a file server is set up with individual user space as well as departmental directories that are limited by access control lists so end users may transfer and store datasets or other data. Unlike the End User Network, the Patient Medical Information System is not accessible to all GIAC employees. The ability to access and update records pertaining to patient information is based on an employee's profession as well as their role in a specific study. Access to patient data is available either by a fixed IP web site available only to the PMIS network or by custom built front ends built specifically to access the SQL database. A major function of the PMIS network is to collect and analyze patient information. Further, GIAC maintains a public website in which the general public may download educational documents and publications without restriction. These sites are only accessible to a number of web programmers as well as the web master.

Assignment 2 Areas of Risk

Every aspect of GIAC's existence revolves around the investigation of cancer and its research. GIAC's staff members spend incredible amounts of time performing tasks such as analyzing chemical compounds used to treat cancer, researching scientific studies to avoid duplication of work and collaborating with researchers around the world to keep on top of new techniques and technologies. The culmination of these efforts results in the collection of cancer-related information disseminated in spreadsheets, databases and documents based on GIAC's research. This collection of data is the "crown jewel" of GIAC. Like other businesses, GIAC is susceptible to various risks. However, the three main risks that are of the most concern are:

1. Compromise of the public web servers.
2. Unauthorized access to the Patient Medical Information Database.
3. Loss of research data and patient information due to virus/malicious software.

Compromise of the public web servers

The information provided on GIAC's public website is used by teachers, students and researchers as well as the general public. GIAC provides various types of information about cancer and cancer treatments through its web site. This information is relied upon to be credible information, especially in regard to research publications. Both abortion activists and animal activists pose the largest threat as candidates for defacing the GIAC web sites. Persons who are opposed to the use of animals for research might want to make their agenda known by substituting their beliefs in place of GIAC's research. They might even alter animal statistics published in online research papers or downloadable data sets. Similarly, the anti-abortionist groups might be under the impression that stem cells are used by GIAC in the advancement of certain types of cancers. They too might want to publish their agenda or modify the hard work of GIAC researchers. In either case, modification or defacement of GIAC websites could tarnish GIAC's reputation. Many people rely on the fact that GIAC will provide accurate information about its studies, animal usage and data so that teachers may teach accurate information, scientists can rely on the sets of data provided by GIAC's site and parents who have a child diagnosed with cancer can find out about their child's specific cancer as well as the latest treatments. Another disastrous effect of losing face is losing funding. If there is skepticism about the studies conducted at GIAC are inaccurate, misreported or have unfounded results, funding for various studies could be pulled from GIAC and thus this part of the organization would suffer greatly.

Mitigation of web server compromise
GIAC houses its external public-oriented web sites on Macintosh-based servers. This serves two purposes. Compared to Microsoft web servers, the Macintosh platform has fewer known security vulnerabilities. Most hacking attempts tend to exploit known vulnerabilities. Since there are fewer known vulnerabilities, the threat should also be reduced. The Lucent Brick 201 also adds another layer to reduce risk since it eliminates packets from external sources to just particular ports. To further reduce the risk of compromise, changes to the web site are monitored by software that tracks and reports content change of the production web sites. Backup of content is maintained on separate media as well as the development servers that are on the End User Network. Computers of employees designated to make changes to the production server may only reach the production web servers in the DMZ. Any other attempt to connect to the production server would be reported by the Real Secure IDS to the network and security administrators.

Unauthorized access to the Patient Medical Information Database
Since GIAC's primary research is on cancer and its treatment, suitable people must be found in order to participate in the studies. Participants' medical data, as well as study data, is maintained in the Patient Medical Information System. Information such as their type of cancer, family cancer history and other demographic information is kept by GIAC in the strictest of confidence. Disgruntled employees, hackers and insurance companies would gain the most by obtaining illegal access to the patient data. Disgruntled employees might want to alter clinical data or results in order to discredit their supervisors or even GIAC in general. They might even want to steal data to extort money from GIAC or sell to insurance companies. If insurance companies hired hackers to obtain access to the data, they would have access to records of patients whose genetic profiles make them candidates for certain types of cancer. Similarly, they might deny a policy to patients who tested positive using a radically new form of cancer detection method that has not yet been approved. The bottom line is that insurance companies would save a ton of money if they knew up front who had cancer prior to issuing a policy. Similarly, hackers who would want to make a name for themselves could take the patient data and plaster it on a public website to show how easily they could compromise GIAC's network. This public exposure would cause GIAC to suffer extremely adverse effects. First, GIAC would be in violation of the Health Insurance Portability and Accountability Act (HIPAA) in which GIAC could be fined for infractions since sufficient security was not in place. Another potential problem as a result of unauthorized access would be lawsuits by participants. Civil lawsuits found in the favor of participants could be costly and may even force GIAC to close. However, the most serious damage to GIAC would be the damage to its reputation and the violation of trust to research participants. Without participants, GIAC would not be able to conduct clinical studies and this would hamper operations.

Mitigation of unauthorized access of the Patient Medical Information Database

Several steps have been taken to limit access to the Patient Medical Information System. First, when converting to an automated system, security was kept in mind and it was determined that placing the network on its own independent, non-routable fixed IP network would provide a certain amount of security from intranet and Internet attacks. Another step taken was to configure every computer so that end users could only run or update their Microsoft Access front end application or use a web browser to get patient data. This helps to minimize potential damage caused by Trojans and viruses since the end user cannot write to the registry or other parts of the hard drive. Another point of unauthorized access could be the single computer that requires access to the Internet for transfer of patient lab data. This computer is restricted by the Microsoft Internet Security & Acceleration Server to make only secure HTTPS connections. The Lucent Brick 201 locks out all external traffic except the contractor's fixed IP address of the lab web server to the dual-homed computer. A personal firewall is used to further protect the dual homed computer from computers on the End User Network by filtering packets that are not from the Microsoft ISA server. This way, only filtered data from the IP of the contractor lab will be accepted by the personal firewall. The data is never written directly to the backend SQL server. Instead, it has a proprietary application that transforms the data to a share that only a special account can write to a file server share on the Patient Medical Information System. The data is added to the backend SQL server by a scheduled job. Another step taken to reduce the risk of unauthorized access is SQL roles and password policies. Only specific users can log into the PMIS. Once logged into the system, end users are limited in their visibility based on their role in a particular study. In other words, a data collector in study A may not see participant data in study B. However, physicians may see all medical data any time in case of medical emergency. Forced changing of passwords with a history limitation is mandatory every 90 days. Prior to receiving their credentials for the PMIS network, end users undergo PMIS awareness training and must sign the "PMIS rules of behavior" document.

Loss of research data and patient information due to virus/malicious software

The most potentially devastating threat to GIAC's "crown jewels" or research is the threat of virus infection through malicious software. According to the 2002 CSI/FBI Computer Crime and Security Survey, eighty-five percent of the respondents reported virus attacks making this the most widely detected form of attack or abuse (Power, 4). Further, more respondents reported financial losses from virus attack than any other type of attack (Power, 10). Types of viruses include boot, worms, macro, file and Trojan horse. All of these virus types can cause GIAC loss through destruction, alteration or theft of research data and patient information. Unsuspecting GIAC employees may have the misfortune of being a victim of a computer virus. Unfortunately, viruses can be launched

through executables in email, opening spreadsheets and documents that contain macro viruses, surfing the net to a malicious site that contains bad code or exploring a floppy disk that contains a boot sector virus that makes them an enormous threat to GIAC. Some viruses may have the ability to place Trojans on a computer so that a hacker could gain control to execute programs and possibly alter, delete or steal data. In addition to the normal threat of destruction of intellectual property, viruses may also cause a denial of service attack by congesting network lines to email service thus slowing or halting business operations. Network congestion that makes unavailable or lack of data integrity caused by viruses could also make it impossible to reach the servers that house patient information, thereby inhibiting treatment and medical care. The motivations for virus writing are varied. Generally the publicity surrounding the distribution and destruction that a virus causes would be all a virus writer desired since her motivation might be to impress friends or earn points in the hacking community.

Mitigation for loss of research data and patient information due to virus/malicious software

In order to reduce the threat of virus attacks on the network, GIAC requires every computer to have anti-virus protection. Since Windows platform computers are more susceptible to viruses, it is also mandatory for them to have the ePolicy Orchestrator agent installed. The exchange email server is required to have a specialized program to scan mailboxes and email attachments. GIAC has chosen Sybari's Antigen for Exchange antivirus software. Configuration of this sever is critical to maintain a grasp on the latest viruses. Anther method GIAC uses to reduce the risk of virus infection is the use of McAfee's ePolicy Orchestrator (ePO) to maintain policy on desktops as well as report computers that are not current with definitions or antivirus software engines. The antivirus policy is unchangeable by the end user and is configured such that should the virus protection be cut off, it would restart within five minutes. Another feature of ePO is the ability to alert the Information System Security Officer and her alternate in case of virus detection. Another tool to help mitigate the effects of Trojans and other viruses is the use of intrusion detection and the firewalls. As new viruses are created, some are designed to exploit vulnerabilities on specific ports. If this is the case, the Lucent Brick 201 can cut off access to the port to which information would travel. The intrusion detection system would monitor the network for suspicious activities such as port scanning. Upon intrusion detection, an alert is sent to the Information Systems Security Officer and the alternate to handle incident response. The final mitigating factor to reduce certain types of viruses is to keep software vulnerabilities to a minimum. By applying security patches on a regular basis, the risk of a virus exploiting the vulnerability is eliminated.

Assignment 3 Evaluate Security Policy

Antivirus policy

An antivirus policy is required at GIAC since its employees spend a large amount of time researching and collaborating using email and the Internet, through which malicious software could be inadvertently or intentionally downloaded and executed. The HHS IRM Policy on Prevention, Detection, Removal and Reporting of Malicious software found at http://www.hhs.gov/read/irmpolicy/0007.html (United States Department of Heath and Human Services) is a well-suited policy for GIAC. This policy, which can be found in Appendix A, was written by the U.S. Department of Health and Human Services (HHS), a federal government organization whose primary concern is public health. Along with the Food and Drug Administration (FDA) and other federal agencies, HHS has regulatory oversight on private industries such as GIAC. GIAC has a more limited scope of public health since it deals exclusively with cancers.

With some scaling modifications and organizational changes to reflect GIAC's organizational structure, the policy would make a great template for the GIAC Enterprise Antivirus Policy. Each section of the policy will be evaluated below.

1. The purpose section of the HHS policy clearly defines the intent of the policy. i.e., it is to set up ways to prevent, detect, remove and report malicious software.
2. HHS does a good job of giving a flavor of the types of threats to their organization in their Background section. However, this section should be updated to reflect threats from Internet web sites such as malicious Java Scripts and ActiveX components.
3. In their scope, HHS is clear in stating that every system, whether new or old, is covered under this policy. Had they been any less succinct, they would have been unclear in their goal to make this policy all-inclusive. GIAC's antivirus policy should cover all systems.
4. According to their purpose, HHS wants to set up policies for prevention, detection, removal, and reporting of malicious software.
    a. Section 4.1 jumps off the path to unauthorized access that should be covered in another policy or under prevention. Since physical access to data and logical access via access control lists is important, GIAC added a point to prevention.
    b. Section 4.2 indicates that each operational division shall take reasonable measures to prevent, detect, remove and report viruses. For GIAC's purpose, this would not be necessary since there are no operational divisions that must carry out specific duties.
    c. Section 4.3 prevention section details what needs to be performed by the operational divisions to satisfy HHS's policy. In section

4.3.5, the policy provides for the installation of antivirus software on the perimeter and servers as well as its centralized management. GIAC would like to take this policy one step further by requiring antivirus software on every computer. By doing this GIAC would reduce the threat of viruses through internet email, surfing potentially malicious sites as well as downloading or installing malicious software.

d. Section 4.4 Detection is well written for what it covers. However, for GIAC purposes, the time limits for updating Antivirus signature files should be changed. This should be more liberal since on occasion, antivirus manufacturers have issues with new signature files and they are not apparent until it is too late. In the fourth point, GIAC would make it mandatory for an unknown virus to be sent to the antivirus manufacturer to investigate when possible. This proactive step will get the ball rolling on creating a signature file for it as well as alert the antivirus community to a new threat.
e. Section 4.5 Removal section does a good job of getting infected computers off the network. One improvement, however, would be to change the HHS undeletable virus policy. In order for a computer with an undeletable virus to be allowed back on the GIAC network, the hard drive must be new or sanitized with a new, clean operating system.
f. Section 4.6 provides for reporting viruses by employees, and IT staff. Since GIAC is not a part of the federal government, reporting to FEDCIRC would not be necessary. Since all GIAC computers would be required to have antivirus software, any machines that have somehow been able to bypass virus scanning or have turned off or uninstalled antivirus protection must be reported to the GIAC's ISSO.

5. The roles and responsibilities section offers a granular approach for such a large organization as HHS. It delegates responsibilities in a hierarchical fashion such that everyone involved knows what role they play. GIAC could use the same hierarchical approach, but delegate responsibilities according to GIAC's organizational structure. On the approval of the chief information officer (CIO), the information systems security officer (ISSO) should have the authority to recommend and change the antivirus management software to limit threats. Further, GIAC employee responsibilities would include verifying that antivirus software is activated and is running the latest definitions. Employees are responsible for attending annual security training from GIAC's IT department. Section 5.4 was added to allow for annual security training and enforcement of policy.
6. HHS is probably obligated to report governmental regulations and legislation that apply it so they included it in applicable laws/guidance section. However this information is not necessarily pertinent to GIAC and was therefore removed from the policy.

7. HHS's information and assistance section provides a way for policy readers to have their questions answered should a part be unclear or if they have suggestions for improvements. GIAC believes this section is important to get both positive and negative feedback on implemented policy since the test of time helps to mold and shape policy.
8. HHS included the effective date/implementation section to document when the policy was enacted. GIAC believes that including the effective date is important because it indicates when the policy was adopted and how long it has been in effect. However, the policy should have a method of being reviewed. By modifying HHS's policy, GIAC added a review clause so that the policy must be reviewed yearly since rapidly changing technology might affect existing policies. This leaves the question of who should review the policy. The Chief Information Officer and the Information System Security Officer shall review the policy annually.
9. In their approval section HHS gives the enactors name, their title and the date approved to show someone in charge put the policy in effect. GIAC agrees management should authorize all policy.
10. HHS included a glossary of terms in order to clarify what their definitions of certain terms mean. This is very important in an ever-changing technological world where terms may be confusing or even viewed differently in other people's eyes. This gives the reader a frame of reference when reading the policy and will be included in GIAC's Antivirus Policy. GIAC did change some of the terms to reflect their views.

Revised Security Policy

GIAC Enterprise Antivirus Policy

July 23, 2002

Table of Contents

1. Purpose

This document provides the policies for preventing, detecting, removing and the reporting of malicious computer software, such as computer viruses. The purpose is to assure that pro-active security measures are taken to prevent malicious software from occurring, to raise awareness for recognizing and immediately reporting the occurrence of malicious software, and to ensure that appropriate action is taken to minimize the consequences of a malicious software attack.

2. Background

Computer systems and communication networks are subject to a variety of threats, many of which have emerged with the enormous growth in the use of personal computers, Local Area Networks (LAN), Wide Area Networks (WAN), and the Internet. Non-malicious threats can be through human error, hardware/software failures, and natural disasters. Malicious threats can range from rational (e.g., obtaining something of value at no cost) to irrational (e.g., destroying information or causing embarrassment). These threats must be adequately addressed through proper controls. In addition, GIAC has an obligation to protect the privacy and security of research data.

Malicious software has the potential to cause harm to an organization through the modification, destruction, or release of information or processing resources, and the denial of critical services. Traditional computer safeguards and malware detection efforts play important roles in the implementation of an organization's malicious software prevention strategy.

Originally, the most common "carrier" of viruses was the diskette, since "sneaker net" was the most common means of transferring software and data between computers. However, all organizations with Internet access are now more vulnerable to viruses. Since e-mail is widely used as a business communication tool, e-mail is a favorite infection vehicle for virus writers. As information systems grow in complexity, effective security safeguards must evolve. Security is enforced through a combination of technical and traditional management methods.

3. Scope

The policy contained in this circular is applicable to all GIAC Enterprise information and infrastructure computing resources, at all levels of sensitivity, whether owned and operated by GIAC or operated on behalf of GIAC. This policy is mandatory for all employees, contractors, and others who process, store, transmit, or have access to IT information and infrastructure computing resources. This policy applies to all existing automated systems and to any new

systems technology acquired after the effective date of this policy. This policy applies to all operating system environments.

4. Policy

4.1 Prevention

The Information Technology department of GIAC Enterprise shall establish access controls that limit or detect access to critical resources (e.g., data, files, application programs, and computer-related facilities and hardware) that help to prevent unauthorized modification, disclosure, loss, or impairment of data.

The IT department shall have change controls, life cycle management procedures, and controls to prevent implementation of unauthorized or risk-inducing programs or modifications to existing programs and thus possible interruption of critical processes.

1. When possible and practical, data should be physically secured as well as secured by access control lists.
2. The IT department must train users about the policy of permitting only authorized software on computers, the possibility of receiving viruses and other malicious software from the Internet. Users shall be trained about the possibility of viruses and other malicious code, on the use of virus scanning tools, about their responsibilities for regularly using these scanning tools, and how to handle and report suspected or actual viral infections. Users shall be informed about the procedures for detecting viruses and limiting the spread of infection.
3. All computers connected to any of the GIAC Enterprise network shall have antivirus software as well as a monitoring agent installed.
4. All software installed on any computer in GIAC Enterprise must have approval from the Information Technology section prior to purchase.
5. Monitoring software shall be set up and configured to maintain policy on all clients on the network.
6. GIAC shall employ firewalls and intrusion detection systems to block unauthorized incoming and outgoing network traffic to protect vulnerable systems and report any suspicious activity on the networks.
7. On the End User Network, anti-virus software definitions must be updated within 48 hours after their distribution.
8. In order to reduce the chance of degraded client performance due to bad signatures, anti-virus definitions must be updated at least 48 hours after the End User Network update.

4.2 Detection

1. The GIAC Information Technology department must use anti-virus software to scan all incoming and outgoing e-mail messages, attachments, and files for viruses and other malicious software. The IT department may, at its discretion, strip certain types of attachments with certain extensions regardless of antivirus detection.
2. Antivirus software must be configured such that all files shall be scanned on access on all computers.
3. The virus scanning software engine shall be updated as soon as the next update is available to maintain currency.
4. Virus scanning results shall be logged, automatically collected and audited by the system administrator or security staff.
5. If an unknown virus is discovered and no cleaning routine is available, the Information Technology department must isolate the virus and keep a copy. A separate copy of the virus must be sent to an antivirus manufacturer for further analysis.

4.3 Removal

1. Any machine suspected of infection by an unknown virus with no known cleaning routine available shall immediately be isolated and appropriate measures shall be taken to remove the virus. If necessary, the machine should be disconnected from all networks. If the virus cannot be removed, the machine shall remain unconnected from the network
2. Off-the-shelf virus scanning tools shall be used to remove a virus from an infected file, program or storage media. If scanning tools still do not remove the virus and the scanning tool manufacturer cannot provide an update in a satisfactory time frame, all software on the device shall be deleted including boot records. The software shall then be reinstalled from uninfected sources and rescanned for viruses. All devices shall be checked carefully for suspected sources and locations of viruses, including any shared network services, programs, e-mail messages, and files. All devices shall be cleaned and rescanned promptly upon discovery of a virus.
3. All the steps taken to recover from a virus infection incident shall be documented. These steps shall be useful as a future reference in updating procedures and educating personnel.

4.4 Reporting

1. Employees shall inform the Information System Security Officer or Information Technology department immediately of any different or out of the ordinary behavior that a computer or application exhibits; they also report any virus detected by their local antivirus application.
2. When informed that a virus has been detected and is likely to be widespread, the system administrator or other designated personnel shall inform all users who may have been exposed to the same programs or data that a virus may have infected their systems.
3. After the confirmation of the existence of a widespread virus, the system administrator shall notify the GIAC's parent IT department's security personnel and potentially infected users of the steps necessary to determine if their system is infected and the steps to take to remove the virus.
4. Reports shall be made of all detections to the Information Technology's CIO on a monthly basis.
5. Reports shall be made of any computer not running antivirus software to the Information System's Security Officer for rectification.

5. Roles and Responsibilities

Information systems security responsibilities and accountability shall be explicit. The responsibilities and accountability of owners, providers of information services, and users of computer systems and other parties concerned with the security of information systems shall be documented.

5.1 The Chief Information Officer (CIO)

The Chief Information Officer (CIO) is responsible for establishing and implementing the information security policies to assure that pro-active security measures are taken to prevent malicious software and to ensure that appropriate action is taken to minimize the consequences of an attack.

5.2 The Information System Security Officer (ISSO) / ISSO Alternate

The Information System Security Officer or an alternate chosen by the CIO to act as ISSO when the ISSO is unavailable is responsible for:

- Monitoring and updating GIAC's security policies, procedures, standards, and architecture to enable better detection and response capability.

- Coordinating responses for incidents.
- Developing and disseminating information concerning the potential dangers from malicious software, guidelines for its control, and serving as a central point for incident reporting, handling, prevention, and recognition.
- Installing or designating staff to perform installation and periodic configuration of antivirus management software tools as threats occur.
- Presenting the annual security awareness training seminars for GIAC staff and maintaining data of staff attendance.

5.3 Employees and Contractors

Neither employees nor contractors may disable or otherwise change anti-virus software on their workstation or other systems without specific authorization, and shall comply with virus prevention activities and report any suspected or actual viruses immediately to the information system security officer or information technology staff. In recent years, there has been a proliferation of hoaxes disguised as virus warnings. These hoaxes are usually transmitted through e-mail and contain messages to send the alert to as many others as possible. They are NOT viruses, but may cause work disruption through false scares or represent a denial of service attack through their proliferation by overloading the e-mail system. All such "virus warnings" should be immediately reported to the system administrator or other ISSO alternated personnel but not forwarded to others. All employees are responsible for either attending computer security training or viewing the online computer security presentation during the month of June each year. After either presentation, the employee must sign a security policy statement that reinforces points made in the presentations. New hires are responsible for completing the online security training and signing the security policy statement prior to getting an email or network account. Employees hired within six weeks of the annual training are exempted from the training.

5.4 Policy Enforcement

Reported violations of this policy shall be documented by the ISSO or the IT staff and reported to the CIO. The CIO is responsible for notifying the Human Resources Department, the employee committing the infraction and their supervisor of the documented violation as well as reporting to GIAC management for enforcement with the prescribed consequences in Table 1. Human resource personnel are responsible for writing formal reprimands and termination notices. CIO is responsible for writing the first warning and denial of network services.

Antivirus Policy Violation Table

Violation	1st offense	2nd offense	3rd offense	4th offense
Removal of antivirus software	Formal reprimand by human resources	Removal of all network privileges for a week	Permanent removal of network privileges / termination of employment if unable to perform job duties.	
Disabling antivirus software	Warning	Formal reprimand by human resources	Removal of all network privileges for a week	Permanent removal of network privileges / termination of employment if unable to perform job duties.
Modification of antivirus software settings	Warning	Formal reprimand by human resources	Removal of all network privileges for a week	Permanent removal of network privileges / termination of employment if unable to perform job duties.
Transmission of Virus hoaxes	Warning	Formal reprimand by human resources	Removal of all network privileges for a week	Permanent removal of network privileges / termination of employment if unable to perform job duties.
Failure to attend or review annual security training presentations.	Disable all network and email accounts until rectified. CIO may temporarily allow medical			

	staff an extension on PMIS network only.			

Table 1

6. Information and Assistance

Please direct questions, comments, suggestions or requests for further information to the Chief Information Officer at (134) 456-7890.

7. Implementation and Review

The effective date of this policy is the date the policy is approved. The policy shall be reviewed every year on its anniversary to determine its effectiveness and to propose changes. The CIO and the ISSO shall perform the review. Changes shall be given to the Director of GIAC for approval and implementation.

8. Approved

_____

Jane J. Smith
Director, GIAC Enterprise

Glossary

Computer Security Incident - an event that may result in, or has resulted in the unauthorized access to, or disclosure of, sensitive or classified information; unauthorized modification or destruction of systems data; reduced, interrupted, or terminated processing capability; malicious logic or virus activity; or the loss, theft, damage, or destruction of any IT resource. Examples of incidents include the insertion of malicious code (e.g., viruses, Trojan horses, back doors);

unauthorized scans or probes; successful and unsuccessful intrusions; insider attacks.

Computer Virus - an executable or self-replicating program spread from executables, boot records, and macros as a set of instructions, and attaches itself to programs, files, diskettes, or other storage media. This set of instructions can then be spread to other programs, files, disks, systems, or networks. The instructions can display a message, erase or alter files, or potentially render a workstation or network inoperable. Sometimes, instead of disruptive instructions, a virus can cause damage by replicating itself and depleting resources such as disk space, memory or network connections. Other threats to user systems include worms, Trojan horses, and logic bombs. Worms infiltrate programs and alter or destroy data, search for open shares to write infected files as well as saturate network bandwidth. A Trojan horse can be a destructive program that comes concealed in software that not only appears harmless but attractive to an unsuspecting user (such as a game or graphic application). Logic bombs are usually timed or event triggered to do damage or stop software from functioning.

Detection - determining that a record, data file, or storage media is contaminated with a virus.

Malicious software - any code that is intentionally included in software or firmware for an unauthorized purpose.

Unauthorized Software - any software that is installed without the approval of the Information Technology Department.

Assignment 4 Develop Security Procedures

Procedure for Initial configuration of Virus Scan v4.51 on ePolicy Orchestrator v2.5

Purpose
This procedure is designed to assist in fulfilling the GIAC Antivirus policy by providing initial configuration settings for VirusScan v4.5 through McAfee's ePolicy Orchestrator. This software will fulfill many aspects of the policy such as detecting, alerting and reporting of viruses. Further the procedure will prevent viruses by centralized administration and scheduling in policy to update antivirus definitions.

Responsibility of Performance and Frequency
Initial configuration may be completed by the ISSO or ISSO alternate. This process is required whenever a new ePolicy Orchestrator server is required on the network due to hardware upgrade or a new independent network is initiated.

Changes may be made by the ISSO or ISSO alternate on an "as necessary" basis.

Actions
Configuring VirusScan v4.51 settings in ePO:

1. Log into ePolicy Orchestrator.
2. Click the GIAC site under Directory in the left pane.
3. Uncheck the inherit check box to set up new configuration settings to inherit through the entire GIAC site.
4. On the policies tab, click on VirusScan v4.51 for Windows.

Each section has tabs that need to be configured as follows:

System Scan Settings
This section sets up what to scan, what to do if a virus is detected, whether to trigger an alert, and what, where and how much to log for reporting. Additional configuration information can be found in Fisher's "*e-policy Orchestrator Walk Through*" at
http://download.nai.com/products/media/mcafeeb2b/pdf/literature/ePOWalkThroughGuide.pdf.
McAfee Antivirus software can employ a heuristic scanner when examining files for viruses. In his article "Heuristic Techniques in AV Solutions: An Overview," Markus Schmall indicates that "heuristic scanning looks for certain instructions or commands within a program that are not found in typical application programs" (1). In heuristic scanning, the antivirus software will look for pieces of code that are typically used in known exploits. The code is compared to a rule system. If a noticeable pattern or sequences of code occur, then a trigger in the detection software indicates a probable infection. Heuristic scanning is important because

it takes antivirus scanning one step further by testing for the unknown based on what is known.

Detection tab

1. Uncheck Inherit box
2. Check Enable System Scan
3. Check the following boxes
    a. Inbound
    b. Outbound
    c. Access
    d. Shutdown
    e. Compressed files
    f. System scan can be disabled
    g. Show icon in the taskbar
    h. Enable heuristics scanning
    i. Select the all files option button
    j. Select enable macro and program file heuristics scanning. Action tab
4. Make sure Inherit is checked. GIAC wants a GUI interface for Windows 9.x users as opposed to a non-GUI. Accepting the defaults ensures that the end user will not be able to access the infected files.

Alert tab

1. Uncheck Inherit
2. Notify alert manager so alerts are sent to ePO

Report

1. Uncheck Inherit
2. All boxes should be checked except session setting <SOFTWRE_INSTALLED_DIR>/VSHLog.txt
3. The size of the log file is 100 kilobytes

Exclusion

1. Uncheck Inherit
2. The box should be empty

Email Scan Options

Using this configuration, messages and attachments arriving at the desktop of a GIAC client will be scanned.

1. Uncheck Inherit
2. The following boxes should be checked/selected
    a. Enable scanning of e-mail attachment
    b. Corporate mail
    c. Microsoft Exchange (MAPI)
    d. All attachments
    e. Compressed files
    f. Enable heuristics scanning
    g. Enable macro and program file heuristics scanning

Download Scan options
This configuration will scan all downloaded files from the Internet.

1. Uncheck Inherit
2. Select enable internet download scanning
3. Select all files, scan compressed files, enable heuristics scanning and enable macro and program file heuristics scanning.

Internet Filter Options
This configuration allows scanning of ActiveX controls and Java applets as well as logging these actions.

1. Uncheck Inherit
2. Select enable java and ActiveX scanning
3. Select default files, scan compressed files, enable heuristics scanning and enable macro and program file heuristics scanning.

Security Options
By enabling a strong password on all sheets, this will make it virtually impossible for settings to be changed by the end user.

1. Enable password protection for all property pages and log its password in a secure file.

Alert Options
This configuration sends messages to the alert manager in case of virus detection.

1. Uncheck inherit
2. Enable Alert Manager Alerting
3. Fill in the IP address for the Destination for alerts.

Configure AutoUpgrade Task
The purpose of auto upgrade is to set the policy on each client to go to an FTP site and check for Antivirus definitions. Definitions by policy must be updated on a daily basis. The FTP site that houses the updates must authenticate with a special user name and password.

1. Select GIAC site in the left pane
2. Click action and schedule new task
3. Select Virus Scan 4.51 for windows and auto upgrade
4. A new task will appear in the tasks pane on the right
5. Double click the task to open it
6. Click settings button
7. Uncheck inherit
8. Fill in the address of the FTP server. (When DNS is not used use IP address.)

9. Uncheck use anonymous and fill in the user name with the appropriate FPT user name
10. Fill in the password. (Place password in secure file)
11. Fill in reenter password
12. Click scheduler tab
13. Scheduled task should run daily local time at 12:00 randomized for two hours
14. To accomplish this select daily under schedule task
15. Under start time change to 12:00p.m.
16. Click local time
17. Check enable randomization
18. Select 2 in the "hours" box
19. Place a 1 in the schedule task daily every box.
20. Click apply and ok buttons

ePolicy Orchestrator Agent

In order for the agent to update, it must have communication with the server. The agent configuration section allows each agent to check the policy every 5 minutes to see if it has changed. Similarly, the agent must maintain contact with ePO. This section will also allow each agent to run without the end user seeing it in the system tray and will let the end user know if reboot is required.

1. Expand directory
2. Click GIAC site
3. Under policies tab expand ePolicy Orchestrator agent
4. Click Configuration
5. Under agent options uncheck show agent tray icon
6. Check prompt user when software installation requires reboot
7. Set the policy to enforce interval every 5 minutes
8. Enable agent to server communication every 15 minutes

Verification of changes

One hour after initial settings or periodic changes are made, the ISSO or ISSO alternate must verify that changes to the settings have propagated to client computers by physically checking the configuration setting of three computers on the network in question. If the changes have not occurred, the ISSO or ISSO alternate must investigate and evaluate why the changes have not occurred.

Appendix A

The following policy is copied verbatim from the following website: http://www.hhs.gov/read/irmpolicy/0007.html (United States Department of Heath and Human Services)

HHS IRM Policy for the Prevention, Detection, Removal and Reporting Of Malicious Software

January 8, 2001

HHS-IRM-2000-0007

Table of Contents

---

1. Purpose

This document provides the policies for preventing, detecting, removing, and the reporting of malicious computer software, such as computer viruses. The purpose is to assure that pro-active security measures are taken to prevent malicious software from occurring; to raise awareness for recognizing and immediately reporting the occurrence of malicious software; and to ensure that appropriate action is taken to minimize the consequences of a malicious software attack.

2. Background

The Department of Health and Human Services' (HHS) security program complies with Federal laws, regulations, and directives and communicates uniform policies for the protection and control of information technology (IT) resources directly or indirectly relating to the activities of the Department. Computer systems and communication networks are subject to a variety of threats, many of which have emerged with the enormous growth in the use of personal computers, Local Area Networks (LAN), Wide Area Networks (WAN), and the Internet. Non-malicious threats can be through human error, hardware/software failures, and natural disasters. Malicious threats can range from rational (e.g., obtaining something of value at no cost) to irrational (e.g., destroying information or causing embarrassment). These threats must be adequately addressed through proper controls. In addition, HHS has an obligation to protect the privacy and security of personal data.

Malicious software has the potential to cause harm to an organization through the modification, destruction, or release of information or processing resources, and the denial of critical services. Traditional computer safeguards and malware detection efforts play important roles in the implementation of an organization's malicious software prevention strategy.

Originally the most common "carrier" of viruses was the diskette, since "sneaker net" was the most common means of transferring software and data between computers. However, all organizations with Internet access are now more vulnerable to viruses. Since e-mail is widely used as a business communication tool, e-mail is a favorite infection vehicle for virus writers. As information systems grow in complexity, effective security safeguards must evolve. Security is enforced through a combination of technical and traditional management methods.

3. Scope

The policy contained in this circular is applicable to all HHS information and infrastructure computing resources, at all levels of sensitivity, whether owned and operated by HHS or operated on behalf of HHS. This policy is mandatory for all Operating Divisions (OPDIVs), employees, contractors, and others who process, store,

transmit, or have access to IT information and infrastructure computing resources in the Department. This policy applies to all existing automated systems and to any new systems technology acquired after the effective date of this policy. This policy applies to all operating system environments.

4. Policy

4.1 Protection against unauthorized access

HHS will assure that its systems and data are safe and secure from unauthorized access that might lead to the alteration, damage, or destruction of automated resources and data, unintended release of data, and denial of service.

4.2 Reasonable measures

Each OPDIV shall ensure that all reasonable measures are taken to prevent, detect, remove, and report viruses.

4.3 Prevention

Each OPDIV shall establish access controls that limit or detect access to critical resources (e.g., data, files, application programs, and computer-related facilities and hardware), that helps to prevent unauthorized modification, disclosure, loss, or impairment of data.

Each OPDIV shall have change controls, life cycle management procedures, and controls to prevent implementation of unauthorized or risk-inducing programs or modifications to existing programs and thus possible interruption of critical processes.

1. As specified in the "HHS Automated Information Systems Security Program Handbook," users shall be trained about the policy of permitting only authorized software on computers, the possibility of receiving viruses and other malicious software from the Internet. Users shall be trained about the possibility of viruses and other malicious code, on the use of virus scanning tools, about their responsibilities for regularly using these scanning tools, and how to handle and report suspected or actual viral infections. Users shall be informed about

the procedures for detecting viruses and limiting the spread of infection.

2. All software and data imported onto computers through physical (e.g., floppy disks, tapes) or electronic means (e.g., e-mail, file transfer protocol [FTP], downloading from the web) shall be scanned before the file is opened and read by the user. All Files shall be scanned prior to opening.
3. Through the use of enterprise infrastructure management tools, software configurations shall be scanned by OPDIVs on a daily basis to validate that no unauthorized software has been added to any computer or server, further reducing the likelihood of malicious software or virus introduction to the network. OPDIVs shall implement the enterprise infrastructure management asset management program registry.
4. Each OPDIV shall employ the prevention technique of isolating or segmenting the network with firewalls to block unauthorized incoming traffic, direct incoming traffic, and protect vulnerable systems.
5. Anti-virus software shall be installed at the network perimeters (e.g., entrances to the OPDIV, at the junctions between OPDIV and Internet, and at other locations if the sensitivity of data and risk of spreading a virus between sections of a network warrant it) and deployed to file servers, e-mail servers, and Internet gateways to limit the spread of viruses within the network. This virus checking shall allow centralized and/or localized virus scanning for an entire organization and reduce overhead by simultaneously scanning incoming messages that have multiple destinations. It also allows for centralized administration of the virus scanning software, thus limiting the locations at which the latest virus scanning software needs to be maintained and updated.

4.4 Detection

1. Each OPDIV shall use anti-virus software to scan all incoming and outgoing e-mail messages, attachments, and files for viruses and other malicious software. Each OPDIV shall scan in real time all network servers.
2. The virus scanning software engine shall be updated when the next update is available to maintain currency. The virus software signature files shall be updated within twenty-four hours of manufacturer's release (unless it is needed immediately for an emergency) with the latest viruses.
3. Virus scanning results shall be logged, automatically collected, and audited by system administrator or security staff.
4. If an unknown virus is discovered and no cleansing routine is available, the OPDIV system administrator shall isolate the virus and keep a copy for analysis.

4.5 Removal

1. Any machine thought to be infected by an unknown virus with no known cleaning routine available, shall immediately be isolated and appropriate measures shall be taken to remove the virus. If necessary, the machine should be disconnected from all networks. If the virus cannot be removed, the machine shall remain unconnected from the network
2. Off-the-shelf virus scanning tools shall be used to remove a virus from an infected file, program, or storage media. If scanning tools still do not remove the virus and the scanning tool manufacturer cannot provide an update in a satisfactory time-frame, all software on the device shall be deleted including boot records. The software shall then be reinstalled from uninfected sources and rescanned for viruses. All devices shall be carefully checked for suspected sources and locations of viruses, including any shared network services, programs, e-mail messages, and files. All

devices shall be cleaned and rescanned promptly upon discovery of a virus.
3. All the steps taken to recover from a virus infection incident shall be documented. These steps shall be useful as a future reference in updating procedures and educating personnel.

4.6 Reporting

1. Employees shall inform the system administrator or other ISSO alternated staff immediately of any different or out of the ordinary behavior that a computer or application exhibits, or any virus detected.
2. When informed that a virus has been detected and is likely to be widespread, the system administrator or other ISSO alternated personnel shall inform all users who may have been exposed to the same programs or data that a virus may have infected their systems.
3. After the confirmation of the existence of a widespread virus, the system administrator shall notify a predetermined list of agency management and security personnel and potentially infected users of the steps necessary to determine if their system is infected and the steps to take to remove the virus.
4. The OPDIV Senior Information Systems Security Officer shall report any incidents to the Department's Senior Information Systems Security Officer and directly, when appropriate, to the General Services Administration's Federal Computer Incident Response Capability (FEDCIRC).
5. OPDIV system administrators shall report to the OPDIV Senior Information Systems Security Officer the quantity and location of machines that bypass the virus scanning. The OPDIV Senior Information Systems Security Officer shall report this information to the HHS Senior Information Systems Security Officer.

5. Roles and Responsibilities

1. Information systems security responsibilities and accountability shall be explicit. The responsibilities and accountability of owners, providers of information services, and users of computer systems and other parties concerned with the security of information systems shall be documented.

2. The HHS Chief Information Officer (CIO)

The HHS Chief Information Officer (CIO) is responsible for establishing and implementing the information security policies to assure that pro-active security measures are taken to prevent malicious software and to ensure that appropriate action is taken to minimize the consequences of an attack.

3. The Deputy Assistant Secretary for Information Resources Management

The Deputy Assistant Secretary for Information Resources Management (DASIRM) is responsible for monitoring and updating Department's security policies, procedures, standards, and architecture to enable better detection and response capability. The DASIRM is responsible for notifying OPDIV CIOs and coordinating responses for incidents that span more than one OPDIV.

4. HHS Senior Information Systems Security Officer

The HHS Senior Information Systems Security Officer is responsible for developing and disseminating information concerning the potential dangers from malicious software, guidelines for its control, and serving as a central point for incident reporting, handling, prevention, and recognition. In addition, the HHS Senior Information Systems Security Officer shall promptly notify the HHS CIO, DASIRM, and OPDIV Security Officers of computer security incidents including the presence of viruses.

5. THE OPDIV CIOS

OPDIV CIOs are responsible for:

establishing and implementing policy, procedures, and practices to assure that OPDIV systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, or destruction of automated resources; unintended release of data and denial of service;

ensuring that all OPDIV employees and other users of HHS IT resources comply with this policy;

ensuring that IT security requirements, procedures, and practices are provided in computer security training materials; and

ensuring that security awareness and training is mandatory for all personnel who use, operate, supervise, or manage computer systems; that new employees receive orientation outlining their security responsibilities; and that program mangers are providing periodic security training (minimum of once a year) to their employees.

6. The OPDIV Senior IT Security Officers

The OPDIV Senior Information Systems Security Officers are responsible for:

promptly notifying the HHS IT Security Officer of computer viruses;

ensuring that appropriate procedures are implemented and instructions issued for the detection and removal of viruses;

ensuring that all OPDIV personnel are aware of this policy and incorporate it into computer security briefings and training programs;

ensuring that anti-virus scanning software engine shall be updated when the next update is available to maintain currency. The virus software signature files shall be updated within twenty-four hours of manufacturer's release (unless it is needed immediately for an emergency) with the latest viruses for the detection and removal of malicious software;

ensuring that when a virus infection is confirmed the extent of contamination is determined; and

serving as a focal point for incident reporting and subsequent resolution.

7. Supervisors and Managers

Supervisors and managers shall ensure that their staffs (Federal and contractor) are aware of their security responsibilities for preventing and reporting viruses, and receive periodic security training.

8. Employees

Employees shall not disable or otherwise change anti-virus software on their workstation or other systems without specific authorization, shall comply with virus prevention activities, and report any suspected or actual viruses immediately to their help desk, system administrator, or other ISSO alternated personnel. In recent years, there has been a proliferation of hoaxes disguised as virus warnings. These hoaxes are usually transmitted through e-mail and contain messages to send the alert to as many others as possible. They are NOT viruses, but may cause work disruption through false scares or represent a denial of service attack through their proliferation by overloading the e-mail system. All such "virus warnings" should be immediately reported to the system administrator or other ISSO alternated personnel but not forwarded to others.

6. Applicable Laws/Guidance

The following public laws and Federal regulations are applicable to this policy circular:

- Computer Fraud and Abuse Act of 1986 (P.L. 99-474);
- Computer Security Act of 1987 (P.L. 100-235);
- Privacy Act of 1974 (P.L. 93-579);
- Clinger-Cohen Act (Information Technology Management Reform Act of 1996 - Division E of P.L. 104-106);
- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Resources,

Appendix III, Security of Federal Automated Information Resources;
- Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, May 22, 1998;
- HHS Automated Information Systems Security Program Handbook, May 1994; and
- IRM Policy for Establishing an Incident Response Capability, HHS-IRM-2000-0007.

7. Information and Assistance

Direct questions, comments, suggestions or requests for further information to the Deputy Assistant Secretary for Information Resources Management at (202) 690-6162.

8. Effective Date/Implementation

The effective date of this policy is the date the policy is approved.

OPDIVs shall have six months from the date of implementation of the EIM tools to fully comply with this policy.

These policies and procedures will not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

The HHS policies contained in this issuance shall be exercised in accordance with Public Law 93-638, the Indian Self-Determination and Education Assistance Act, as amended, and the Secretary's policy statement dated August 7, 1997, as amended, titled "Department Policy on Consultation with American Indian/Alaska Native Tribes and Indian Organizations." It is HHS' policy to consult with Indian people to the greatest practicable extent and to the extent permitted by law before taking actions that affect these governments and people; to assess the impact of the Department's plans, projects, programs and activities on tribal and other available resources; and to remove any procedural impediments to working directly with tribal governments or Indian people.

9. Approved

_____/s/_____ _01/08/01__

John J. Callahan
Assistant Secretary for Management and Budget

Glossary

Computer Security Incident - an event that may result in, or has resulted in the unauthorized access to, or disclosure of, sensitive or classified information; unauthorized modification or destruction of systems data; reduced, interrupted, or terminated processing capability; malicious logic or virus activity; or the loss, theft, damage, or destruction of any IT resource. Examples of incidents include the insertion of malicious code (e.g., viruses, Trojan horses, back doors); unauthorized scans or probes; successful and unsuccessful intrusions; and insider attacks.

Computer Virus - an executable or self-replicating program spread from executables, boot records, and macros as a set of instructions, and attaches itself to programs, files, diskettes, or other storage media. This set of instructions can then be spread to other programs, files, disks, systems, or networks. The instructions can display a message, erase or alter files, stored data, or potentially render a workstation or network inoperable. Sometimes, instead of disruptive instructions, a virus can cause damage by replicating itself and depleting resources, such as disk space, memory or network connections. Non-virus threats to user systems include worms, Trojan Horses, and logic bombs. Worms infiltrate programs and alter or destroy data. A Trojan Horse is a destructive program that comes concealed in software that not only appears harmless but attractive to an unsuspecting user (such as a game or graphic application). Logic bombs are usually timed or event triggered to do damage.

Detection - determining that a record, data file, or storage media is contaminated with a virus.

Malicious software - any code that is intentionally included in software or firmware for an unauthorized purpose.

Unauthorized Software - any software that does not have a certificate of authority to operate.

References

Fisher, Lee. “e-Policy Orchestrator Walk Through.” 4th revision. December 2001. URL: http://download.nai.com/products/media/mcafeeb2b/pdf/literature/ePOWalkThroughGuide.pdf (9 July 2002)

Lucent Technologies. “VPN Firewall Brick 201.” 28 September 2001. URL: http://www.lucent.com/livelink/0900940380004b3b_Brochure_datasheet.pdf (16 July 2002)

Microsoft Corporation. “Internet Security and Acceleration Server 2000.” URL: http://www.microsoft.com/isaserver/evaluation/productguide_v1.1.doc (13 July 2002)

Power, Richard. “2002 CSI/FBI Computer Crime and Security Survey.” Spring 2002. URL: http://www.gocsi.com/pdfs/fbi/FBI2002.pdf (9July 2002)

Schmall, M. “Heuristic Techniques in AV Solutions: An Overview.” 4 February 2002. URL: http://online.securityfocus.com/infocus/1542 (16 July 2002)

United States Department of Health and Human Services. “HHS IRM Policy for the Prevention, Detection, Removal and Reporting Of Malicious Software.” Revised 29 August 2001. URL: http://www.os.dhhs.gov/read/irmpolicy/0007.html (3 July 2002)

Last Updated: July 25th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Oslo Autumn 2017	Oslo, Norway	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
Community SANS Banff MGT512	Banff, AB	Oct 23, 2017 - Oct 27, 2017	Community SANS
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
Community SANS Memphis MGT512	Memphis, TN	Nov 06, 2017 - Nov 10, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced