



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

## Interested in learning more?

Check out the list of upcoming events offering  
"Introduction to Cyber Security (Security 301)"  
at <http://www.giac.org/registration/gisf>

**DELIVERING A SECURE MISSION-CRITICAL OPERATING PLATFORM TO THE  
U.S. MILITARY**

**GIAC INFORMATION SECURITY OFFICER  
PRACTICAL ASSIGNMENT v1.2**

**DANIEL\_MELLEN\_GISO.DOC**

**SUBMITTED MAY 2, 2002**

## TABLE OF CONTENTS

<b>GIAC Enterprises – Overview .....</b>	<b>3</b>
GENERAL DESCRIPTION .....	3
IT INFRASTRUCTURE .....	3
INFRASTRUCTURE DETAILS BREAKDOWN:.....	4
BUSINESS OPERATIONS .....	7
<b>GIACENT– Security Risk Assessment .....</b>	<b>14</b>
3 SIGNIFICANT RISK AREAS .....	14
<i>GIACENT’s “Crown Jewels”</i> .....	14
<i>Power to the People</i> .....	16
<i>Putting barbwire on the fence</i> .....	19
<b>Evaluate and Develop Security Policy .....</b>	<b>22</b>
<i>Security Awareness Training For All Employees</i> .....	22
<i>Policy Assessment</i> .....	23
REVISED SECURITY POLICY .....	25
<i>Security Awareness Training Policy</i> .....	25
<b>Develop Security Procedures.....</b>	<b>28</b>
<i>Procedure to setup employee profile and requirements in Policy Center</i> .....	29
<i>Procedure for employee to execute training and learning assessment module</i> .....	31
<b>Bibliography .....</b>	<b>34</b>
<b>APPENDIX.....</b>	<b>37</b>
FIGURE 1: GIACENT NETWORK TOPOLOGY .....	38
FIGURE 2: GIACENT SECURITY INFORMATION CLASSIFICATION .....	39
FIGURE 3: GIACENT ASSET DETAILS .....	39

## **GIAC Enterprises – Overview**

### ***General Description***

GIAC Enterprises (GIACENT) is a government research and development agency responsible for the creation of the Secure Operating Environment (SOE), a semi-open source platform for military, mission-critical systems. In addition to this main initiative, they are responsible for the development of in-house and approval of vendor applications to be run on the SOE.

GIACENT's success is dependent on several variables. These variables include the development of commercial applications for the SOE, in-house development of applications, enhancements to the SOE and upholding the reputation of the operating system and its suite of approved applications in the military domain. The success of the agency is directly proportional to the success of these factors.

The main driver for GIACENT is the satisfaction of the Government with their products. In order to support their business operations, GIACENT must maintain its good standing with the high-ranking officials that are in charge of approving budget allocations. Therefore, losing the trust of the system end-users (generals, battle commanders, etc.), as a result of a breach of security, would potentially cause the agency to be decommissioned.

Since GIACENT's creation in mid-1998, there have been several successful releases of the SOE. Additional application development, both government and commercial, is currently taking place to support and increase its functionality. While increasing the functionality of the platform, GIACENT is committed to maintaining a high level of security standards for themselves and their partners, as much as possible.







GIACENT's system integration engineers install the SOE and approved applications on location, typically at bases and remote military installations. All of the Armed Forces use the operating system for their real-time battle, battle-simulation and information messaging purposes. Technology and innovation are cornerstones of GIACENT's success as well as an impeccable track record of delivering secure, compliant systems. GIACENT has very few competitors in its operating space. This characteristic is very attractive to agency executives and every step to maintain this statistic is taken.

Similar to any organization, GIACENT has several key business functions including: finance, accounting, procurement, human resources (HR), information technology (IT), development & deployment (D&D), and facilities. These divisions are located in the Washington D.C. headquarters and provide the business and employee support as expected in a traditional business.

### ***IT Infrastructure***

The IT infrastructure provides connectivity for all GIACENT operating locations and partner organizations involved in collaborative SOE application development. The IT team includes servers, enterprise applications, client support for GIACENT employees and contractors using the corporate applications, desktops, the helpdesk, operational security, network, and data.

See [Figure 1 in the Appendix](#) for a network topology diagram of the GIACENT agency's infrastructure. The red and green lines show the static egress routes of communications through the border router to the DMZ from the public Internet and to the PN for remote users over the Virtual Private Network (VPN). The Internet and Remote Users are shown as separate clouds simply to make a logical distinction between the two. The following is a legend reference for the network diagram and it outlines the main components of GIACENT's topology:

Symbol	Device	Device description/function
	Router	Provides isolation, forwarding, and traffic direction between LAN and WAN segments of GIACENT's network (border and internal).
	Firewall	Provides filtering and service blocking. It is also a means of fault-tolerance for the border router.
	Firewall & VPN	Provides filtering, blocking and remote Virtual Private Networking (VPN or V) access for GIACENT employees to the protected network (PN).
	Hardened Component	Means that additional steps have been taken to secure this device.
	Intrusion Detection System	Intrusion detection element used for notification as well as configuration testing and review by GIACENT security engineers (host & network).
	Hardware Firewall	Introduces diversity and redundancy into the security architecture.

### **Infrastructure details breakdown:**



Hardware Manufacturer/Model: Cisco 12004 / Integrated Services Adapter for VPN <sup>[24]</sup>  
Software: IOS 12.2

Configuration: Deny ICMP redirects, deny un-routable (private) addresses, and deny spoofed addresses for border router. Additional filters are added as needed to support business requirements and special incidents. Demilitarized Zone router: (DMZ) allow only port 25, 80, 53 and 443 traffic for mail, web and resolution services from Internet interface only. PN router allows encrypted VPN traffic from Remote Access firewall only and only permits access to the left branch of the protected network. All routers have Tripwire installed to monitor changes to any configuration files. Integrity checks are run as needed.



Hardware Manufacturer/Model: Nokia BIG-IP Fireguard HA + 540 <sup>[13]</sup>

Software (Configuration): Nokia IPSO 3.4.1; (1) Checkpoint 4.1 SP5 with security patches for DMZ; (2) VPN-1 & Checkpoint 4.1 SP5 with security patches for PN

Configuration: The Nokia has the high availability configuration applied for corporate Internet access, 3 interfaces each (incoming, outgoing, mgmt)

Default rule sets include:

DMZ-Standard-Outgoing Side: Allow management traffic, drop all to firewall, allow port http, dns, https, vpn to specific IP address, drop all.

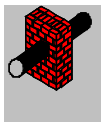
DMZ-Standard-Incoming Side: Allow management traffic drop all to firewall, allow only traffic to specific IP Addresses based on apps (http, dns, https, ssh, scp, app specific), drop all.

PN-Standard-Outgoing Side: Allow management traffic, drop all to firewall, allow vpn to specific IP address, drop all.

PN-Standard-Incoming Side: Allow management traffic drop all to firewall, allow only traffic to specific IP Addresses based vpn, drop all.

Nokia Rule base for firewall: Allow management, allow firewall mgmt, drop all to firewall.

Corporate Internet access policies (http, https, imap), Drop all. <sup>[0]</sup>



Hardware: Nokia Firewall/VPN Product <sup>[13]</sup>

Software: IPSO 3.4.1

Configuration Specification: Provides a combination of Firewall and VPN services.

Default rules: Runs Contivity Stateful Firewall Engine. Maintains a table of registered MAC addresses for which giacent.mil laptops have been issued. Uses Nortel's group password token authentication to verify user. This authentication scheme is part of the standard issue installation for all GIACENT mobile users and is a one-way encrypted password token.



Hardware: Nokia IP650 <sup>[26]</sup>

Software/Configuration: IPSO 3.4.1; ISS RealSecure Network Sensor 6.0.1 <sup>[2]</sup>; signatures updated regularly and applied according to OS, centrally managed console.

Provide network based Intrusion Detection (NBIDS) and are strategically located at points on the network where monitoring is desired. In many cases NBIDS are used to monitor and test component configurations. For example, NBIDS are located on either side of most of the firewalls and routers in GIACENT. This allows network and firewall administrators to implement a rule set on a firewall and then use the NBIDS to monitor the packets and insure that only the desired traffic is making it through the firewall.



Hardware: Varies

Software: Varies; ISS RealSecure Server Sensor 6.0.1 for servers<sup>[2]</sup>; signatures updated regularly, unused ports blocked against malicious traffic, Tripwire 2.4.2

Configuration: Represents a system or component with a heightened or additional security considerations. One such example is all systems within the DMZ – each of these systems are equipped with a host based intrusion detection systems (HBIDS). The DMZ systems have also been hardened and penetration tested to improve their security. Systems inside the DMZ only host applications and services absolutely required for their intended function and all other services are disabled or deleted. Risk considerations are driven by the sensitivity of the data delivered and the amount of damage that is possible given a compromise. In addition to the DMZ systems, other systems on the GIACENT PN that house critical data, employee data, procurement and facilities operation information, which are critical to the company's business continuity, are protected. These systems all contain AV clients, HBIDS (above) and are scrutinized by thorough penetration testing conducted by the operational security team. In addition, Symantec Security Operations<sup>[10]</sup> Center's 24 hours/day X 7 days/week program is employed on these machines. In addition, many machines within environments (see asset matrix in Appendix) have Tripwire installed to monitor changes to any critical files. Integrity checks are run as needed.



Hardware: SonicWall Pro 300<sup>[36]</sup>

Configuration: Provides additional layered protection of hosts and enterprise applications for users of the GIACENT PN and remote access. This hardware firewall is intended to diversify the security of the network and provide a redundant solution to protecting GIACENT's resources and assets. Having this layered approach to securing the most sensitive and valuable information can have benefits that are unrecognized at design time. For example, a recent vulnerability in the SNMP protocol<sup>[31]</sup> was announced and faulty systems were identified. Having a manufacturer diverse security implementation can provide the necessary protection while a fix is developed. This component has VPN technology included in the appliance and supports up to 1000 Security Associations. All settings required to support a single VPN channel constitutes a Security Association. Essentially, this represents the maximum number of simultaneous SonicWall VPN connections that can be supported at any one time.

For any authorized users accessing GIACENT remotely:

Hardware: Agency issued laptop hardened by NSA hardening guide.<sup>[18]</sup>

Software: Windows 2000 SP2, IE 5.5, MS Office 2k Pro SR2

Symantec Antivirus<sup>[10]</sup>

Nortel Networks Extranet Client v2.62<sup>[37]</sup>

Tiny Personal Firewall 2.0.15A<sup>[27]</sup>

PGP Freeware 7.0.1 for data encryption/signing<sup>[28]</sup>

Asset Management software

See the GIACENT Asset matrix ([Appendix – Figure 3](#)) for low-level details of systems.

Configuration: All service packs for operating systems and applications applied. GIACENT Nortel Group token authentication settings install; Default browser configuration: Security Settings Local-Low, Internet – Medium, NSA recommended security policy applied<sup>[18]</sup>

### ***Information Classification process defined:***

At the suggestion of a National Security Agency (NSA) best practices document<sup>[35]</sup>, GIACENT systems were divided by information type and associated criticality level. They devised a (13) thirteen-layer classification hierarchy, which is evaluated based on Confidentiality, Integrity and Availability (CIA). This multi-layer security architecture ([Figure 2 – Appendix](#)) was developed through a collaborative self-assessment with the team leads, discussed below.

By working against a standard framework for security architecture, where systems are assessed and secured based upon data classification and business importance, GIACENT enjoys what Fred Kerby calls “Defense in Depth” as described in his coursework from section 9.5 of SANS Information Security Officer 2002 training textbook. The information stored on GIACENT systems was classified and ranked from most critical to least critical as can be seen in a few examples below.

Sensitive mission-critical data has the greatest implications on business continuity, agency effectiveness, and information importance for GIACENT. This includes the source code for the SOE and applications developed in-house. One, often overlooked, piece of critical data is the backup. Host and network backup data is extremely valuable because it could effectively be the archived contents of GIACENT’s most coveted live information. If backup data is not secured to the highest degree, a replica of the agency’s crown jewels could be reconstructed and all of the effort deployed to protect the live version would be nullified.

At the other end of the spectrum is mailing list information and non-sensitive information; both information types have low ratings for the CIA categories. One example of this type of data is GIACENT static web content. This series of .html pages is strictly informational and provides no real functionality to their web presence. Other items pertaining to physical security, such as their facility drawings are somewhat more valuable and fall in the middle of the information type range.

### ***Business Operations***

GIACENT is comprised of several highly specialized teams of people. There is a Security Advisory board, operational security team, development team, requirements team, testing/integration team, help desk engineering team and finance and human resource team. Some of the roles and responsibilities are common amongst the more technical teams and there is some team overlap and rotation in personnel between these teams. These groups’ cooperation and efforts combine to allow GIACENT to function as a business unit.



## ***GIACENT Employees – Roles and Reliance***

GIACENT employs roughly seventy-seven full-time people. The breakout of these employees, by team looks something like the following:

Advisory board	10
Development	15
Information Technology	32
Operational Security	12
General IT	08
Help Desk	12
Testing/Integration	10
Finance/Accounting	04
Human Resources	04
Procurement	02
Total	77

These figures are only estimates because, as indicated above, in the more technical teams, people have the opportunity to shift onto different teams to satisfy work-variety and business-needs requirements.

The Development and Testing/Integration folks spend a majority of their time in the isolated SOE development / testing / production environment evolving and testing the latest and greatest features and enhancements to the SOE. These groups deal with data in the highest ranked criticality information type sections (SOE Source Code & Application Source Code). Much of the work that they perform is done so on the SOE platform as well as Linux and Solaris workstations. This relies heavily on the configuration management and version control pieces of the GIACENT infrastructure as well as the UNIX workstation support experts from the Helpdesk group.

The Advisory Board primarily works on the administrative and strategic elements of GIACENT. Their work is done on Windows machines under the IT umbrella. These people rely heavily on E-mail, World Wide Web access, and desktop applications such as Microsoft Office at the Washington DC headquarters. They spend time developing the training requirements, reviewing partner applications, reviewing proposals and requests for development from vendors. This group of individuals relies heavily on the mail and dns services provided in the DMZ as well as the desktop and application support experts in the Helpdesk group.

The Helpdesk subteam is responsible for knowing, understanding and troubleshooting all of the components of the GIACENT infrastructure for its employees and partners. These individuals rely on process and troubleshooting applications that aid them in their daily work. They also are reliant on the GIACENT developers and system testers who are responsible for writing the technical documentation surrounding the SOE. This information is valuable when inquiries from partners are received regarding the PIS or in house Partner Lab. This group uses many of the built in management features of the GIACENT infrastructure to assist them in their routine troubleshooting tasks.

The General Information Technology team relies on nearly the entire GIACENT infrastructure throughout its tasks, as well. The operational security subgroup within the IT team focuses a significant amount of its time on the proper and accurate functioning of the DMZ housed and access control pieces (firewalls, routers, etc.). This subgroup is responsible for monitoring and testing the implementation of the GIACENT network, which includes all of the hardened systems as well as the HBIDS and NBIDS. Important components such as the PIS and Partner Labs fall under the jurisdiction of the IT team and require constant monitoring and maintenance. The IT team receives input from the Helpdesk and works in conjunction with them to solve internal and external problems as they arise.

The Finance, Accounting, Human Resources and Facilities Teams exclusively run Windows 2000 systems and applications (SAP-ERP) and rely on the desktop support experts on the Helpdesk team. These users also enjoy the benefits of Email and World Wide Web browsing and rely on the DMZ housed infrastructure. Since some of these teams have a web presence and applications on the GIACENT Intranet, they rely on the proper functioning of departmental domains on the network and the ability of employees to access their web spaces. This dependence is split between the Helpdesk and the IT teams – typically the Helpdesk is required to troubleshoot the problem and the IT team is called upon to actually implement a fix for the problem.

Business partners are only granted access to two pieces of the GIACENT Infrastructure (aside from the obvious publicly accessible Email and WWW services), namely the PIS in the DMZ and the isolated Partner Integration Laboratory in the confines of the Washington DC headquarters. These two components are secured very well and are under regular scrutiny by the operational security team. These partners also rely on the Helpdesk for any problems that are encountered during application testing in both of the abovementioned pieces.

As can be seen in these breakouts, different teams within GIACENT are dependent on different elements of the agency's infrastructure. However, in order for GIACENT to function successfully as a unit, all of them must be operating as intended. This is a significant undertaking and requires the cooperation, communication and commitment of all of the teams within GIACENT.

Essential business operations include the following core items:

1. Public facing information and functional servers including everything in the DMZ: Web Server, DNS Server, Mail server and Partner Integration Server (PIS). These systems are managed by a few of the DMZ specialists on the operational security team. For obvious reasons, there is a sizeable emphasis on security for these systems. The primary function of the web server is information and content publishing; its purpose does not have a large functional or operational element to it, with the exception of the authentication to the PIS. A high-speed, read-only CD-rom stores all static web content for GIACENT and is pushed out to the web server every 20 minutes through the PIS. This measure makes an embarrassing defacement much more challenging and ephemeral. The absolute maximum amount of time that a defacement could ever be present on the GIACENT web

site would be 19 minutes and 59 seconds. These steps were taken because GIACENT is not the target of everyday script kiddies, but rather focused, funded, and primarily anti-United States groups.

2. The PIS is provided to allow GIACENT partners to system/integration test their applications on the most current SOE release as well as download any signed and encrypted patches/hotfixes. The users are authenticated once they have logged into the web server and only then will be allowed to communicate with the integration environment. This is done using Windows 2000 Kerberos authentication over SSL with client and server certificates. Access arrangements and certificate exchanges are made once partners are certified and accredited (discussed below) to simplify patch download and lab access. There is a special application that allows encrypted file transfer (using scp) to the integration environment. A script running on the integration server processes the specially packaged software and installs it on the PIS. This same application allows for the secure (ssl) observation of application results. This allows development shops to run preliminary tests on their applications to verify the results before coming to the Washington integration lab to do a full-blown system test.
3. The headquarters facility where the majority of the GIACENT operations occur is physically located in the heart of Washington, D.C. It houses all of the GIACENT core technical systems, as well as all of the administrative and operational systems. These include IT, HR, finance, accounting and procurement. A few of the departments have small intranet web spaces. For example: HR is in charge of VigilEnt's Policy Center application <sup>[6]</sup>, which runs on a web server where the content and application is under their control. All server-grade systems that are logically positioned in the GIACENT Protected Network (PN) are physically located in the data center in Washington. There are many additional security measures that have been taken to ensure that access to the machines on this part of the GIACENT network is only granted to authorized persons through the intranet or VPN. Access to the IT data center itself is a two-phase technique whereas authorized users have IBG retinal scans stored in a database <sup>[34]</sup> and also swipe their magnetic badges.
4. GIACENT has built an isolated partner integration lab where partners can come to the GIACENT Washington facility and test approved releases of their applications on the SOE. In the network diagram, this lab is shown as a single server/database combination; however, this is just for conceptual purposes. This lab is actually five sets of network segregated database/server duos allowing five different application-programming shops to be testing their solutions simultaneously. The reason this lab is provided and might seem redundant to the partner integration combination provided in the DMZ is twofold. The first is that this lab is fully supported by the engineering and tech support staff. The second reason is for the protection of the development companies; this separation provides security for proprietary data for competitors. GIACENT realizes that in order for it to be successful there must be applications built to increase the functionality of their platform. For this reason, they have attempted to make it easier for developers and integrators to work with the operating system and support staff. There is a CD-rom backup attached to this system, which contains a ghosted image of the environment to allow for a quick refresh of used systems. This same CD-rom system is used to load vendor applications to be tested in the lab environment. There is a strict policy prohibiting the connection of non-GIACENT machines to the network.

5. The certification and accreditation (C & A) of SOE development shops is a process that application development vendors go through in order to be approved to develop applications that will be tested and potentially run on the SOE. There are several aspects to this process including: company and employee background checks, secure software development lifecycle (SDLC) verification and various other legal and contractual details. Once an organization has completed the C & A process, they can participate in GIACENT issued requests for proposals (RFP) or they can submit an intent to develop (ITD). In the first case, organizations bid on a piece of work, outlining their credentials and detailing previous work experience from which they can leverage experience. In the second case, an organization essentially requests permission to develop an application for use on the SOE. Once an organization has won a bid on a piece of work or has their ITD approved they are granted access to the partner integration setup in the DMZ, are supplied with the SOE and supporting applications' application programming interfaces (API) and are able to schedule access to the partner integration lab in the Washington, D.C. facility. This last step only occurs when they an organization is submitting an application for final review and integration. Most of the process occurs over GIACENT's secure web site (described above).
6. GIACENT's Advisory board agrees with Glen Sharlun "security through obscurity is no security at all." <sup>[20]</sup> For this reason, an open source SOE forum (OSSOEF) was established when GIACENT opened its agency doors in 1998. This forum includes some of the security industry's most respected experts who review the operating system code for potential programming or design flaws. Each of these individuals holding this highly esteemed position have obtained top secret Department of Defense (DOD) clearance, have signed a non-disclosure agreement (NDA) for reviewing the SOE source and all acquiesce that GIACENT's mission is prudent and in the best interest of the United States military. The typical review session is held at the D.C. location to which members of this board are transported. The duration for the first review was a little over three and a half weeks, however, only impacted code is reviewed for future releases and the normal length of a review varies on the amount of new and affected material, averaging less than a business week. GIACENT believes that this scrutiny is highly beneficial in helping to build the highest quality and most secured system.
7. The operational security team who has direct contact with GIACENT's help desk and support staff in case any problems arise does deployment of operating systems to military posts. The installation package is created using bit-arts' InstallWrap software <sup>[33]</sup> that simplifies the install while allowing interactive instructions on the new or enhanced features included in the latest release. These deployed installations occur approximately once every, on a schedule, shortly after the April 20th release.
8. In-house development and testing of SOE and supporting applications are other major business operations. Environments are present to allow for the rapid development and deployment of new and updated code for all of GIACENT's software. The SDLC for the SOE takes approximately 1 year to complete. This schedule is widely communicated to vendors and is accounted for in their development cycles. This means that each year, around the 20<sup>th</sup> day of April, GIACENT deploys a new version of their secure operating system API to current and newly subscribed government agencies who require the use of it. Incorporated into the SOE are a few bit-arts products called Softlocx and Crunch <sup>[33]</sup>. Softlocx integrates copy protection at the development language level so that the code

cannot be reproduced easily. The Crunch application restricts the ability of an unseasoned cracker from de-compiling the application into source code. These two integrated applications are another layer of defense in the SOE development and deployment model. Included in the realm of in-house development are hot fixes and patches. In the event that a security vulnerability is discovered by GIACENT testers or SOE end users, code that addresses the vulnerability must be quickly developed and tested before exploits can be developed to take advantage of the problem. Both hot fixes and patches are deployed through GIACENT's secure web site.

9. Development process – P Version Control System (PVCS) is an industry standard versioning and configuration management system used to deploy code to developers and is handled on an as needed basis. Code is checked out, worked on, and returned for integration. This code is stored in the production system and is very well protected by tools such as Tripwire, a HBIDS, etc. There is one off site CD-rom copy of the latest release of the source code in a safe in a DoD basement in Washington; this disc is considered top secret - critical. This copy is used as a secure backup in the unlikely event of a catastrophic problem. There are three main system architectures for which the SOE and its supporting applications are built. The first is the RISC architecture, the second is the x86 or Intel architecture and the third is the sparc architectures.<sup>[4]</sup> These systems were chosen because they are the most widely used architectures by military forces.
10. The GIACENT helpdesk and SOE technical support engineers are available 24/7 via phone, email, chat and web conference. There is a core group of individuals that are full-time helpdesk support and then there are other members who are on a rotation from another logical teams in the agency. The full time help desk team is provided with extensive product and security training. This training is usually enough to qualify the employee for at least one of the recommended certifications. For qualified individuals, GIACENT will cover the cost of the certification exams. To provide task variety for GIACENT employees, a role rotation was developed that allows people to learn different aspects of the business. For example, a developer that has been coding for several months and has completed his/her current task might rotate to the security team and help work with the intrusion detection team. Another example is a tester who, following a SOE release, wanted to try something new and could rotate to the helpdesk to assist with the support function. There is constant training and information sessions put on by each of the teams to create a level of awareness and allow people to begin developing skills in various areas.
11. GIACENT offers VPN access to their PN. This access is strictly administered and is only offered to internal employees. The typical users of this service are off-site HR, finance, facilities or IT people. As discussed above, strong authentication is employed using group password token authentication through Nortel's extranet client and the MAC addresses of all users with VPN access must be registered. GIACENT attempts to implement flexible work arrangements to allow their employees to have a reasonable work-life balance. This service greatly facilitates this ability and increases the productivity of off-site employees. Source code and some other GIACENT proprietary data is not accessible from this entrance. These small networks are isolated in the PN and are updated and patched using a CD-rom.
12. The Security Advisory Board and Operational Team – There are two major players responsible for the evolution and maintenance of the security posture at GIACENT and

they are the security advisory board and operational team, respectively. These two groups work on separate elements of the same complex problem – protecting GIACENT. The security advisory board is responsible for defining the critical systems of the agency and recommending mitigating actions. On the other hand, the security operational team is responsible for assessing the feasibility and implementation of the proposed actions. These two groups work very closely to ensure that the security controls implemented at GIACENT do not hinder business operations, but rather, enable its progress. The security advisory board is composed of seasoned system administrators, various team managers and executives from within GIACENT, as well as a few esteemed members from the Security Community. This means that team is mix of system owners, data owners and business process owners, complimented by legal, HR, finance and unbiased outside influences. The goal of the Security Advisory Board is to sculpt a solution of least risk to propel a security enabled development process and platform for the GIACENT agency. Among the initiatives of this group are:

- Policy creation
- Metrics reporting
- Security stewardship
- Training plan creation and evolution
- Monitoring & Enforcement of policy and training requirements
- Future GIACENT security Posture
- Overall SDLC risk reduction

Sanctioned by the director of GIACENT, the security advisory board has direct influence on policy enforcement, issue escalations and incident response allowing for minimal negative impact on the agencies day-to-day operations. The operational security team provides low-level program implementation and management support for the Advisory Board. The Advisory Board holds monthly meetings to discuss general concerns, as well as make decisions regarding training waivers and exceptions, along with dealing with current events and issues raised since the last meeting.

13. A problem that has plagued the computing community from its inception is operating system developer's inability to produce a secure and functional platform. For this reason, the details and source for the SOE is very valuable and must be protected. While the SOE is open source to a select group of experts in the security community for their evaluation and scrutiny, it is not disseminated to the general public because of its military application. This balance of openness and obscurity is very delicate but very necessary and has proven to be very successful.
14. The facilities team's responsibilities include the physical location: buildings, furnishings, climate control, waste management, cleaning and physical security. One of the first lines of defense for GIACENT is the physical security layer. This encompasses access to the GIACENT buildings, laboratories and anywhere that their network connectivity is accessible. In addition to the general areas of interest, more specialized areas such as, network equipment rooms, server closets and the main data center all fall under their restrictive domain. A guard shack, at which point a GIACENT badge must be shown regulates the entrance to the GIACENT locations. Building badges are distributed with new employees' welcome and orientation packets. Persons requiring higher security clearance must apply for such access and be pre-approved by their team lead, team manager and team operational security officer. Employees granted access to these areas must complete a more extensive amount of training before their badges are approved and activated.

15. Finance, HR and procurement don't warrant in depth discussion because their function within GIACENT is no different than any other traditional corporation. Standard activities such as hiring, firing, promoting, purchasing and bookkeeping are among their main tasks.

Note: The details of the SOE will not be provided in this document. If this occurred and the wrong people got their hands on it (read: Microsoft), the unemployment rate amongst security technologists everywhere would skyrocket.

## **GIACENT– Security Risk Assessment**

The three most critical security risks for GIACENT are outlined here and specific details of the impact and consequences to this agency, in particular, are discussed below.

1. GIACENT maintains a reputation for producing a secure operating system and suite of applications; this fact makes them a target for persons trying to tarnish their name out of quest or spite. GIACENT is currently the only secure platform that delivers functionality to mission critical military systems and thus has significant intellectual capital in the form of proprietary software – their proverbial “crown jewels.”
2. People are the second greatest risk to the success and business continuity of GIACENT. Social engineering is an age-old method for gleaning sensitive or privileged information from unsuspecting employees. The only means for combating this type of exploitation is awareness. Another aspect of the people equation for GIACENT is retention. The agency employs a large concentration of skilled developers and must remain current with compensation plans so as to keep these developers content and employed at the agency.
3. GIACENT uses VPN and Internet based technologies for some business-to-agency transactions with its partners and remote users. These areas from a considerable risk to the reputation and livelihood of the agency because these are the most popular as well as vulnerable avenues that could result in eventual access to the GIACENT PN.

### **3 Significant Risk Areas**

#### **GIACENT's “Crown Jewels”**

The source code for the SOE is, by far, the most valuable commodity that GIACENT possesses. The risk facing the agency is the unauthorized distribution of this code. The design and source for the SOE is very valuable and must be protected. There are several players in the Government market and operating system development sector that would pay an enormous sum of money to get their hands on it. There are two logical means for this happening. The first is an intruder penetrating the GIACENT PN and pulling out the source. The second, and harder to protect and predict, is the insider threat – someone on the inside accepting a bribe or payout to deliver the code. This threat is particularly difficult to predict because you must have a certain level of trust with your employees but at the same time you have to be sure that they are worthy of such trust. Of course, background checks are performed on all GIACENT employees, similar to, but more stringent than the checks that are administered for potential partners.

The consequences of the distribution of the source code would be detrimental to the agency's existence. No longer would GIACENT be the sole owner of this code and no longer would the military be the sole operator of a secure, mission critical operating system. The trust relationship and proprietary agreement between GIACENT and the United States Government would be dissolved. GIACENT could potentially face legal ramifications because the disclosure of this source code puts many military systems at risk.

The external threat requires that the intruder actually gain some form of physical access to the GIACENT Washington DC facility. Potentially, a scam could be formulated where a cracker poses as a legitimate facilities worker and gains unauthorized access to a network closet where critical infrastructure components are housed. Once this physical access is obtained, the cracker could infiltrate all resources accessible from the infrastructure available to him and eventually locate the source code version control system (PVCS). The intruder could then deploy a brute force attack on the CM system and eventually gain access and checkout code, disguised as a normal developer.

The multiple potential avenues for an internal threat is much more difficult to prevent. For example, a developer could accept a bribe or be the subject of a blackmail effort. This developer might slowly, over the course of several months or years, check out and locally store (or hide) code until nearly all or enough of the code could be taken offsite and given to the unauthorized persons behind the plot.

Several mitigating steps could be employed by GIACENT to further ensure the safekeeping of their SOE code. Exhaustive logging and auditing of code check in and check out should be instituted. There should be a set of defined procedures for accessing any of the operating system code and the rule of least and need-to-know privilege should be implemented. The smallest amount of code required to complete a given task should be allocated to a developer. This would create restrictions on the amount of code that can be checked out by any developer at one time.

In addition, restrictions on the hours at which code can and cannot be checked out would limit the time of day from which a would-be attacker would have to gain unauthorized access. There should also be smart trending and anomalous activity monitoring so that developers cannot check out the entire code base, piece by piece, without raising a flag in the system. Another procedure that should be instituted is that no code can be downloaded onto a local share. All programming, review and compilation should be done on a remote drive and the check in process should remove and "wipe" the area from which it is checking the file in. This means that the shared, network area is wiped clean of any data so that so called "dumpster diving" cannot occur.

An alternative possibility would be the off site location of SOE code. To combat the external perpetrator, a honey pot could be established with code that resembles the SOE source, when in actuality it is not. This diversion would provide a delay in the cracker's process and might allow more time for intrusion detection systems to pick up on the unauthorized access. Along the same lines, the code could be stored remotely and transmitted encrypted when needed over a dedicated, secure line. This would require infrastructure changes in the current GIACENT network topology but would provide another layer of defense.



The cost of exploitation to GIACENT in the context of the SOE source code is enormous. The cost of an unavoidable high profile legal battle is a large, tangible element, while the loss of reputation and embarrassment that would result is a non-quantifiable piece. If the SOE code was discovered it would give insight to the perpetrator as to the inner workings of the platform, likely to aid in identifying weaknesses. Even worse yet, if the cracker was able to modify the code without the knowledge of GIACENT and embedded a Trojan horse, it would be making all future releases of the SOE to military posts extremely vulnerable. This could have very grave consequences and ultimately cost peoples' lives. For instance, if the US were in a battle situation and commanders were unable to use the SOE to communicate between squadron leaders because someone had figure out a way to Denial of Service attack the machine, men and women in the field could be killed. Or if battle secrets were broadcasted through a Trojan horse or other mechanism the outcome could be catastrophic.

This particular risk has a moderate likelihood of occurring, but an extremely high impact and potential for damage.

The severity of possible consequences to the GIACENT crown jewels obviously warrants the utmost attention and all security precautions applied. In essence, it is a matter of national security because, if discovered, US military operations would be comprised.

## **Power to the People**

Of the 3 elements in the security triad <sup>[19]</sup>, the People extension provides the most diverse as well as the most vulnerable area. Technology and process are elements under which stringent controls can be placed and there are known relationships. With people unpredictability and uncertainty are introduced and the exact results cannot easily be assumed. An agency can have best practice procedures and policies in place and have locked down all of their technology but with people in the equation, the weakest link in the security chain is quickly exposed. The Security Awareness area in the SANS Reading Room reiterates this fact with dozens of references to periodicals and studies where the breakdown in security lies at the fault of the people. One example is a February 2001 SANS reading room article <sup>[7]</sup>, which states "It does no good to have firewalls, intrusion detection software and anti-virus software if employees give the key to the door to anyone who asks." GIACENT employees need to be aware of these tactics and receive sufficient training to equip them with the knowledge of what to do when put in a social engineering situation. In the words of John Palumbo, SANS reading room contributor, "The first thing that absolutely needs to be accomplished is training, training, and more training." <sup>[9]</sup> The lack of security awareness training represents one of the highest risks to GIACENT.

GIACENT has several public facing outlets. One is the Helpdesk. Because this service is provided to facilitate partner application development, practically anyone with the correct phone numbers, fax numbers or other contact information could attempt to socially engineer these employees. GIACENT field representatives responsible for the deployment of these systems travel to the military installations where the SOE is implemented. These persons could be targeted by would be attackers both from a physical (SOE media theft) standpoint and a

psychological (conversation on a plane or in an airport) standpoint. These team members should be aware of this possibility and trained to detect it.

Because of the proprietary nature of GIACENT's business and the importance of their information to national, military security even internal employees must be trained on the tactics that they might encounter at social functions or by acquaintances. For example, an HR representative should not divulge information to anyone regarding the method with which he connects to the GIACNET intranet over the VPN. While only limited access could be gained through this attack by potential wrong-do'er, information is power and the more information a cracker has about the operations (i.e. gained from the IT portion of the intranet) the more dangerous she can be. It is not unheard of for a cracker to plan and wait to escalate her access or forge an attack until she knows exactly what she is up against and exactly where the crown jewels are stored. Small bits of information that seem unimportant by themselves can be pieced together to explain more than meets the eye.

For example, say a well thought out attack is waged on GIACENT through an unsuspecting HR representative. An anti-American group has one of its female members involved in a relationship with a male GIACENT HR representative. Say this woman pretends to be fairly computer illiterate and asks to use the HR rep's laptop on occasion to check her internet Email or surf the Web. If the HR rep is not trained that possible social engineering attacks can come from **anywhere**, this could result in a large problem. If this cracker gained unauthorized access to the GIACENT intranet via the HR rep's VPN connection and installed a rootkit or backdoor in the VPN components of the firewalls and routers this could open up a world of opportunity. This cracker could then gain access to procurement and see what software version control management and configuration management products have been purchased, as well as hardware and security equipment. In addition, it is possible that network topology diagrams and facility diagrams could be stolen from the IT and Facilities group. All of this information can be combined to form list of vulnerable entry points and a layout of GIACENT agency for an eventual physical breach to the GIACENT facility and the theft of the GIACENT crown jewels.

The basic reason that the lack of training and awareness for GIACENT employees poses a major risk for the agency is that all of the security measures employed across the board can be circumvented by one person just trying to be helpful. It is human nature for people to want to help people in need. Someone calls the helpdesk and explains that they are locked out of their system and needs to have his/her password reset to get information for a presentation that is about to start, the knee-jerk reaction is to reset the password to avoid embarrassment at the presentation. If the password is reset, without verifying that user is who they say they are, the embarrassment for GIACENT is potentially much greater than just looking unprepared for a presentation.

A few of the consequences of a lack of adequate security awareness training for users of any systems include:

- Theft of GIACENT proprietary information
- Downtime due replication of malicious code such as viruses
- Destruction of data due to execution and replication of malicious code
- Exposure of sensitive, financial or proprietary information

- Financial fraud

The actual consequence of untrained and unaware employees is only measurable on a case-by-case basis. A sophisticated cracker with good social engineering skills could talk a rookie help desk engineer into disclosing the off-site location of the SOE source code. With this information and enough time a cracker could access GIACENT's most valuable assets and could lead the demise of the agency or extortion.

Given the increases in this type of attack, this particular risk has a high likelihood of occurring and a large range of impact and potential for damage, as seen in the hypothetical example above. A cracker's motives range from looking to use the computational power that GIACENT possesses to launch an attack on another company and tarnish GIACENT's reputation in the process, to the desire to steal SOE trade secrets and force the agency to be dissolved or replaced, to decreasing the effectiveness of US military operations. Acceptance and enforcement of policies, combined with security awareness training is imperative in order for GIACENT to be successful at implementing a layered security approach and preventing such attacks from jeopardizing the agencies existence.

Recommended steps to mitigate the risks associated with the lack of a security awareness program to include:

1. Development of a training schedule for all employees as well as a framework for new employees. Awareness seminars should be built into the function of the security group and memorandums and posters should be placed in common meeting areas (cafeteria, break rooms, lounges).
2. Technical and functional review of the security policies and procedures with a panel of users from different groups (finance, accounting, HR, development, IT) and security officers to ensure feasible and realistic guidelines are in place. As Fred Kerby said at the March SANS GISO session "Security should not hinder your business operations, it should be an enabler." The insurance of that point is the goal of this review.
3. Annual security review courses will be administered at which attendance is compulsory. At these sessions, the highlights of securing GIACENT's most valuable items will be reiterated. (GIACENT IT SECURITY DAY)
4. Pre account policy review – Before a user is granted an email or enterprise account, the user must review and sign the related policies: email acceptable use, Internet acceptable use, etc.
5. Periodic (monthly) security awareness messages should be placed on the company intranet site. These messages should contain a tip, an incident that employees can relate to and/or upcoming training session information.
6. Ensure that the security group is in alignment with the GIACENT Security Advisory board's objectives and activities,

The cost associated with these mitigating actions can only be addressed if the details of the solution are stated. As an example, assume that the timeframe is one year; the following rough figures would apply to the above stated actions (time = variable depending on the salary of the employee attending – assume an average of \$40.00/hr):

1. Development of a training schedule for all levels of the agency = \$8,000.00; Awareness seminars and posters = \$15,000.00;
2. Review of the security policies = 40 hrs x 8 people (3 security, 5 random sample) = \$13,000.00
3. Annual security review 2 hours = \$4000 (assuming 50 employees).
4. Pre-account review = \$300 (assuming 3 major policies to review @ 15 min each and 10 new employees a year).
5. Awareness messages - \$0.00
6. Ensure alignment with Advisory board- \$0.00

Another risk identified by the agency is retention of their developers. It is obvious in looking at the CERT vulnerability lists that good developers, capable of producing solid, secure code are at a premium. For this reason, GIACENT developers are paid very well in comparison to the marketplace and HR is constantly doing analysis to ensure that GIACENT is an attractive place to work for these people. The potential consequences of people leaving are a breakdown in the quality of the SOE product and knowledge transfer to a potential competitor. The cost of losing a good developer is very difficult to quantify, however, the cost to analyze current compensation trends works out to be about 10 hours quarterly for an HR representative.

### **Putting barbwire on the fence**

GIACENT has adopted VPN and the Internet based technologies as a cost saving, partner-enabling platform, as have many corporations have done in recent years. The public Internet virtually extends the GIACENT network indefinitely. An increasing trend has been noticed by CERT<sup>[31]</sup> (who logs incidents and vulnerabilities) that there is up to 80% more Internet based attacks this year than last year. This means that this is the entryway of choice for attackers and should not be taken lightly by the agency. The perimeter is the first line of defense for GIACENT; agency executives and military leaders alike say that it should be one of the most secure borders on the Internet. The greatest threat of entry is seen at this point in the GIACENT architecture given that this “front door” is available to anyone with an Internet connection; they are all able to rattle the handle to see what happens.

This risk is especially important to GIACENT for two reasons, the first is business partner application development continuity followed by upholding the reputation of GIACENT as having a genuine interest in security. Because of the frequency and popularity of these types of risks, they pose a greater threat than some other risks that might have a greater impact but have a much lower likelihood of occurring.

Because of the small size of the GIACENT agency and development team, they are highly dependent on the development of vendor applications to be run on the SOE. Part of the integration and testing process occurs in the DMZ through the PIS. It is in GIACENT's best interest to maintain a high level of availability and integrity to this environment so that the external developers do not have difficulty testing and integrating their software with the SOE. If the level of effort required to integrate their application with the SOE outweighs the benefit gained from having it included, they will likely seek opportunity elsewhere.

GIACENT's reputation is a very important commodity to the agency. The trust and belief held by the military community is required for GIACENT's continued success in the mission critical platform space. If the agency is not seen as placing their own security in high regard, then military support and respect for their products will not be maintained.

The specific consequences of a perimeter breach are two-fold. The first implication is the potential disruption of the integration and testing process for GIACENT's business partners. For instance, if the World Wide Web server in the DMZ is compromised by a phf attack, followed by the PIS server through a brute force attack, crackers could disrupt the partner integration/testing process. Access to the PIS server affords attackers the ability to alter the functionality of the GIACENT homegrown application that processes packaged software intended for integration. An attacker could modify the output delivered to the business partner so that it falsely indicated problems with the application or misreported application results. If this were the case, development teams might schedule a time in the Washington DC Partner Integration Lab much earlier than they would actually be ready for or conversely, spend large amounts of time reworking interfaces and code to achieve the proper results from the PIS, when in fact their code was functioning properly to begin with. If attackers were able to implement these changes, it could discourage partners from developing for the SOE due to lack of returns on investment and GIACENT's ability to increase the functionality of the SOE would diminish. This result would, over time, affect the happiness of the military with the GIACENT product and might cause the Government to seek out other commercial vendors offering more functionality.

The second implication of a perimeter breach is the destruction of the reputation of GIACENT as a security focused agency. GIACENT would be unable to maintain its position as a developer of a secure operating system and application if they were unable to secure their own front door. No military or Government in their right mind would support an agency's product, which has responsibility for battle critical functions, if they had a history of perimeter breaches, regardless of how small the impact such breaches had on the product which was delivered. At the same time, if business partners saw that GIACENT was being defaced or had reports of perimeter breaches, they too might reconsider the business viability of GIACENT and focus their efforts on other more stable and secure opportunities, reducing their own risks. As mentioned above the decision-making, high-ranking military officials who are in charge of the purse strings' impression of GIACENT as an agency focused on security is vital to its success. This negative publicity and lack of trust could cause the agency to be decommissioned, despite the fact that it has no real affect on the security of the SOE or it's supporting applications.

Moreover, The inability of the GIACENT security operational team to establish a secure perimeter include some of the same consequences realized if someone gains entry through social engineering, detailed above. A frightening prospect of unauthorized access into the GIACENT PN is that if the perpetrator is able to get in undetected, is he/she able to remain there undetected? The hope is that this would not be possible. In the unlikely event that this is possible, the attacker could wait until a critical moment in time, i.e. a battle situation, and expose all of the agency's proprietary information. Surely this would be detrimental to the military operation as well as the agency's operation overall. Another less important, but reputation affecting concern is that GIACENT could be used as a "zombie" in a dDoS attack, as was perpetrated on Yahoo, eBay, Cnet, e\*Trade and a host of other online companies last year.

These attacks affect other sites as well: “Internet traffic slowed by as much to 26 percent,” according to Net performance watcher Keynote Systems.<sup>[12]</sup> The impact of this negative publicity could tarnish GIACENT’s name in the security realm with its business partners and the military, its financial supporter.

There are also legal issues that are beginning to be raised regarding the liability of companies to protect their systems. GIACENT could be held liable if they were compromised and then used as a resource in an incident against another system or network of another organization. Legal precedence is pointing to negligence and/or joint liability for a malicious act. While the use of GIACENT resources as a zombie is not definitively fatal to the agency, a large legal battle might not be sustainable or in the best interest of GIACENT’s future. In this situation, the Government might choose to decommission the agency to help defend their position. Seeing as this among the most popular and likely present-day attacks and the ramifications to GIACENT’s business operations if successful, this risk is of great concern to the Advisory Board at the agency.

Actions to create a secure perimeter include:

1. Ensure firewalls and routers have filters and rule sets defaulted to the Principle of Least Privilege (PoLP) and only allow known applications and sources. Content screening, user authentication, access control lists, and automatic alerts should also be implemented where possible.
2. Implement all patches and service packs as soon as they have been thoroughly tested. Administrators should monitor security lists<sup>[15, 31]</sup> to keep up to date on known vulnerabilities and their fixes.
3. Test VPN technology to ensure encrypted network traffic streams for mobile users are secure and functioning properly.
4. Implement time based and two-factor authentication technology like ACE servers and SecurID cards from RSA<sup>[1]</sup>.
5. Regularly audit (manually) NBIDS and HBIDS as a learning, awareness and alert mechanism.<sup>[27]</sup> This can be implemented using a co-relational engine to monitor infrastructure devices and would help automate the security analysis.
6. Test the configuration of perimeter security and IDS on a regular basis, as described in “Improving the security of your network by breaking into it” by Dan Farmer<sup>[30]</sup>. This exercise not only improves the security of the site, but it also asks as a teaching tool for the person administering it.
7. Implement fault tolerance (redundancy) at the border router stage.

The cost estimate for securing the first line of defense for GIACENT is mainly an issue of the operational security team’s time. The cost of acquiring networking and firewall equipment is irrelevant because the agency already owns it. The maintenance associated with the staff required to support the infrastructure and incident response team is where the cost is realized. This task is definitely not to be taken lightly. It was best said by Greg Shipley in his 1999 article “Anatomy of an Intrusion Detection” when he stated, “The crackers have the easiest task. They need find only one open doorway; the defenders must check every lock.”<sup>[14]</sup>

The three main risks to the GIACENT agency are like the last three pieces to a puzzle. An exploitation of any one of them will lead to the crown jewels, the completion of the puzzle for

the cracker. GIACENT should work hard to disadvantage would-be crackers by implementing defense in depth, making it difficult to gain unauthorized access and hoping the assailant loses interest, seeking an easier target.

## **Evaluate and Develop Security Policy**

The following policy is the SANS GIAC Information Security Officer (GIAC-GISO) 2001 coursework, “LIONS and TIGERS and LAYERS (of security)” authored by David McLeod <sup>[0]</sup>. This policy is intended to address the issue of training and awareness for the GIAC Enterprises employees.

“

## **Security Awareness Training For All Employees**

### **1.0 Purpose & Overview of Threats**

The purpose of this policy is to establish the standard for security awareness training required for every individual utilizing GIAC-E information systems. Security begins with each person knowing the behaviors required maintain a safe and secure computing environment and the benefits of doing so. Insufficient security awareness training results in a severe set of consequences to the GIAC-E computing systems. As examples,

- Degraded performance of applications and Internet access due to use of unauthorized software or launching of viruses,
- Release of personal logon ids, system passwords, and company confidential information to outside parties,
- Damage and loss of company confidential information contained in GIAC-E computers,
- Easy access to GIAC-E systems by unauthorized persons, inside and outside of GIAC-E,
- Poor public perceptions of GIAC-E, which could result from the above actions.

### **2.0 Scope**

This policy applies to all persons, employees and contractors, utilizing any GIAC-E computer system or application.

This policy applies to all GIAC-E locations including the locations of remote workers.

### **3.0 Policy**

Every person must complete security awareness training on an annual basis. The topics of the training include, but are not limited to:

1. Social Engineering tactics and defenses
2. Password best practices – selection and proper use
3. Securing your computer and workspace
4. Identifying and reporting incidents

Training is administered using a web-based, self-paced training tool called Policy Center. Completion of the training module requires that you complete the instructional module and learning assessment module, which will record your score. Security awareness training is

complete when a passing score is accomplished for each module. Only passing scores will be recorded. There is no time limit for the modules of the training.

#### **4.0 Actions & Responsibility**

For employees and contractors – Comply with security awareness training requirements within the scheduled timeframes for the subject content specified on an annual basis.

For the Security Council – Make recommendations for training schedules, subject content for the entire company, special content for unique business units and workgroups, and review metrics for course completion. Review exceptions and appropriate changes or recourse to manage exceptions and deviations from this policy whenever required. Escalate exceptions to business unit managers and Corporate Compliance Committee as necessary.

For the Information Protection team – Provide on-going administration of the Policy Center tool to ensure high quality content, and systems availability. Provide timely maintenance and update of all Information Protection policies.

For the Corporate Compliance Committee – provide guidance on the applicability and enforcement of this policy.

#### **5.0 Enforcement**

Failure to complete security awareness training in the timeframe specified will result in loss of systems access until training is completed.

Failure to apply the training concepts as part of your daily workplace behaviors could result in disciplinary action up to and including termination of employment.

#### **6.0 Definitions**

Policy Center - Web based policy review and training tool from VigilEnt.

Security Council - core team of business unit representatives responsible for enterprise-wide security stewardship in accordance with the corporate objectives for Information Protections.

Corporate Compliance Committee – team of corporate officers responsible for key business processes and activities of GIAC-E.

#### **7.0 Revision History**

Initial Revision 1.0 – 12/20/01 Author: David McLeod

“ [0]

#### **Policy Assessment**

This policy adheres to the provided metrics of a good security policy. This policy is readable, has clear intentions and the focal issue is apparent. In addition, the audience is specified, the steps to address the problem are laid out plainly and reason this policy has been established is apparent. In April 2002 the FBI and Computer Security Institute (CSI) released a new set of survey statistics for 2001 indicating that: “Ninety per cent of the approximately 500 people who responded ...detected computer security breaches within the last year, with 85 % reporting financial losses as a result and 44 % willing to name a dollar figure, for a total loss of \$455.8-



million (U.S.)<sup>[16]</sup>.“ These figures place both an importance and a cost on security measures across the board.

Although good by the suggested metrics, the completeness and effectiveness of this policy are questionable. There are several areas that could be expanded to help justify the policy to the reader. People are more inclined to follow a procedure or accept change if they understand why they are being asked to do so. There is a fine line between enough and too much information in a policy – the intent is not to get away from the issue being addressed, but to backup with examples or statistics the restriction being imposed. Another noteworthy aspect of this policy is detail. While the policy must be an overarching document that allows for procedural and topic adjustment without having to re-write the entire policy – the policy must clearly define at least the boundaries in which the procedures have scope.

The following are the top few items that should be modified in order to make this good policy great:

1. There needs to be a definitive time limit on the completion of the awareness training. The policy states that the training is to be administered over the web and can be done at the employees pace, with no time limit mandated to complete a module. This would suggest that an employee only need start the training process and they would satisfy that condition.
2. A process for extension needs to be addressed. There needs to be a discussion stating what happens to employees who are not successful in completing the training in the timeframe indicated.
3. More specifics need to be applied for contractors in terms of the timeframe in which the training must be administered. As a general rule they should be treated as employees and abide by the once a year renewal. In the very least, security training should be mandated at the start of every new contract with the exception of a new contract starting within 3 months of previous contract ending. Moreover, a shorter completion time must be indicated for short duration projects or short stint contractors can avoid completing it (or even starting it).
4. The failure to complete the training needs to have ramification levels for the respective number of failures. In the first case, the first offense might warrant a verbal reprimand, the second offense a personnel file/performance, and the third offense, termination or demotion.
5. A good idea is to have incentive for the employee. The addition of a metric in an employee's performance evaluation geared toward successful and timely training completion is an example. Other ideas might be to have an agency-wide competition to see which team can complete their training first or with the highest correct answer average. Positive results can be obtained when people take an interest in something that relates to their career advancement or has the perception of a competition.
6. One missing area in the policy is accountability and responsibility. This policy begs the question, “Where does the buck stop and who is responsible for enforcing the checks on completion of the training?” Some level of management should be identified as the monitoring agent of the training completion and the party responsible for enforcing the consequences of non-compliance should be mentioned.

7. The scope should be refined to include all persons that could affect the safety of the company's operation – There have been cases where janitors were socially engineered into allowing criminals access to facilities<sup>[11]</sup>. As stated in Sandi Smith's article on "The Risks and Rewards of Information Security Planning:" "To increase the success of an information security program, the entire company should be involved and responsible for corporate security."<sup>[8]</sup>

## **Revised Security Policy**

### **Security Awareness Training Policy**

#### **1.0 Purpose & Overview of Threats**

The purpose of this policy is to establish the standard for security awareness training required for every individual on GIACENT property or using, in any way, GIACENT information systems. Security begins with each person knowing the behaviors required maintain a safe and secure computing environment and the benefits of doing so. Insufficient security awareness training results in a severe set of consequences to the GIACENT computing systems and agency.

Examples of potential problems for GIACENT include:

- Degraded performance of applications and Internet access due to use of unauthorized software or launching of viruses
- Release of personal logon ids, system passwords, and company confidential information to outside parties
- Damage and loss of company confidential information contained in GIACENT computers
- Easy access to GIACENT systems by unauthorized persons, inside and outside of GIACENT to perform malicious actions on or using GIACENT resources
- Loss of business partner interest in developing supporting applications for the SOE
- Loss of reputation for GIACENT and more importantly, funding, which could result from the above actions.
- Government seeking other vendors to provide services offered by GIACENT

As can be seen in the above examples, without proper training and awareness, GIACENT's viability as a government-supported agency is at stake. Awareness is a key element in mitigating possible risks in this area. In order for an employee to be effective at thwarting attempts at unauthorized access through social engineering and other means, they must be aware of the signs that indicate this behavior is taking place. For example, if an HR representative working for the agency is unaware of social engineering techniques and divulges the location of network closets in the Washington DC facility to an inquirer in a seemingly normal conversation at a social function, they could, unknowingly, be putting GIACENT at considerable risk to a physical access attack. This procedure is the first step in a process attempting to eliminate the success of this type of attack on agency employees.

The actions of every employee involved in the day-to-day operations of GIACENT are vital and every decision should be made with the best interest of GIACENT and security in mind. The

success of the agency and America's battle critical operations are in the hands of GIACENT's employees and should be handled accordingly.

## **2.0 Scope**

This policy applies to all persons, employees and contractors, who are permitted on GIACENT property or are using any GIACENT computer system or application.

This policy applies to all GIACENT locations including the locations of remote workers.

GIACENT Security Advisory Board members are exempt from this training due to their immense involvement and understanding in this subject matter. Through their development and evolution of the security program they should receive sufficient review of material and concepts. Additional training should not be required.

## **3.0 Policy**

Every person must complete security awareness training on an annual basis and schedules should be synced up with the January 1<sup>st</sup> recycle date, detailed below, whenever possible. The topics of the training include, but are not limited to:

1. Social Engineering tactics and defenses
2. Password best practices – selection and proper use
3. Securing your computer and workspace
4. Identifying and recognizing potential attacks and attackers
5. Reporting incidents and preserving evidence

Training is administered using a web-based, self-paced training tool called Policy Center. Completion of the training module requires that you complete the instructional module and learning assessment module, which will record each participant's score. Security awareness training is complete when each module has been reviewed. All scores will be recorded in the learning assessment module for administrative and incentive purposes only. Training completion dates are stored in each employee's performance feedback form, in his or her personnel file, in the Human Resources department.

### **Full & Part time employees**

The training modules must be completed within 2 months of the employee's start date or March 1<sup>st</sup>, when applicable. Any employee who has not successfully completed security training and has been employed at GIACENT for 6 months or longer should be considered for immediate termination.

### **Contractors**

Contractors should follow the Full & Part time employees' requirements wherever possible. For short-term contracts, or multiple short-term contracts, exceptions can be made. If a contractor works on a contract, which is less than 2 months in duration, an exception or reduced training requirement can be requested. If a contractor starts on a subsequent contract that begins within 4 months of the prior contract ending, a waiver can be requested. All waivers and exceptions must get majority approval from the Security Advisor board, which will decide on such matters during their monthly meeting.

## **Facility & Miscellaneous**

A special training program has been created for this category of employees. It is an abbreviated set of training modules dealing with concepts more pertinent to their roles. It is assumed that Facility and Miscellaneous persons would not require access to the GIACENT network or applications, but that these employees might be targeted for social engineering attacks because of their knowledge and physical access to certain areas. The training modules must be completed prior to the employee's start date. Agencies from which some employees in this category are hired are aware of these restrictions and it is built into preexisting contracts.

## **4.0 Actions & Responsibility**

For employee, contractor, facility and miscellaneous persons – Comply with security awareness training requirements within the scheduled timeframes (January 1 – March 1, or 2 months from employee start date) for the subject content specified on an annual basis or according to above guidelines.

For Team leads responsible for performance reviews of subordinates – Ensure that all direct reports have completed their security training and that their status is up to date on their performance feedback form by March 15<sup>th</sup>, prior to the April 25<sup>th</sup> and September 25<sup>th</sup> annual and semi-annual review processes, respectively or 2.5 months following an employee's start date. A rolling, compiled report is to be submitted to the Security Advisory board by each team lead for their respective team members on April 10<sup>th</sup> and September 10<sup>th</sup> prior to the review processes.

For the GIACENT Security Advisory Board – Develop and evolve training schedules, subject content for the entire company, special content for unique business units and workgroups by December 15<sup>th</sup>, and review metrics for course completion by December 15<sup>th</sup>. Review exceptions, waivers and appropriate changes or recourse to manage exceptions and deviations from this policy whenever required. Perform annual review of personnel files to ensure compliance with the reporting detailed in this policy during the end of April and September employee performance review periods. For deviations and non-compliance, see enforcement section below for action items.

For the Information Protection team – Provide on-going administration of the Policy Center tool to ensure high quality content, and systems availability. Provide timely maintenance and update of all Information Protection policies, when required.

This policy should be communicated from the top down. Support from the (authoring) Security Advisory Board should be apparent to the leads of each of the GIACENT teams. In turn, team leads should impose and reiterate the importance of this policy and training to the individual employees. The importance of this policy and its enforcement should be patently obvious from the executive level at GIACENT. A memorandum containing this policy and all updates should be issued containing the endorsement of the entire GIACENT Security Advisory Board at the start of all employment contracts (during orientation) of new employees and annually, on January 1<sup>st</sup>, when the mandatory training cycle restarts for all current employees regardless of start dates (seek an exception from the Advisory board, if timeframes overlap). A reminder memorandum should be issued at the halfway point of the training cycle (February 1<sup>st</sup> or 1

month following employee's start date) for the employees' time management benefit. Training and updates to this process, pertinent to an employee's role, should be apart of an employee's orientation session and training for new roles should be administered at promotion time.

## **5.0 Enforcement**

Failure to complete security awareness training in the two month timeframe specified for a learning assessment module will result in loss of systems access until the process below is completed.

In the event that an employee fails to complete a learning assessment attempt they can petition for an extension on the module(s), the standard extension period for all employees is two (2) weeks regardless of their category, unless the Security Advisory Board recognizes special circumstances grants a longer period of time. If an employee requires more than two extensions for a single learning assessment module, a meeting must be setup with this employee, their manager and the GIACENT Security Advisory Board to assess the problem and the Board will reach a decision on how to proceed.

Failure to apply the training concepts as part of your daily workplace behaviors could result in disciplinary action up to and including termination of employment.

## **6.0 Definitions**

Policy Center - Web based policy review and training tool from VigilEnt.

Security Advisory Board - core team of representatives responsible for enterprise-wide security stewardship in accordance with the corporate objectives for protecting GIACENT.

## **7.0 Revision History**

Initial Revision 1.0 – 04/09/2002 Author: Daniel W. Mellen

## **Develop Security Procedures**

*Assumptions: The GIACENT Security Advisory Board has developed a level to mandatory training matrix for each level in the agency. Policy Center application from VigilEnt<sup>[6]</sup> has a set of training modules that are aligned with the plans set by the Advisory Board. HR personnel have received training on the use of Policy Center and understand what is responsible of employees at every level (indicated by the matrix).*

The following procedures combine to form the Security Awareness Training policy:

- 1. Procedure to setup employee profile and requirements in Policy Center**
- 2. Procedure for employee to execute training module and learning assessment module.**
3. Procedure for managers to monitor and verify training; for HR to monitor managers to ensure compliance.
4. Procedure for employee training module extension.
5. Procedure for disciplinary action for module non-completion.

\* These procedures will be detailed below

All steps within these procedures should be carried out to their exact specification; the GIACENT Security Advisory Board must approve any deviations, in writing. These procedures have been developed using some of the industry's best practices – sets of proven steps to make effective policy implementation easier. To ensure that GIACENT obtains similar results, it is very important that these procedures are strictly followed. Deviations from these procedures could result in a compromise to GIACENT systems and therefore should be taken seriously.

## Procedure to setup employee profile and requirements in Policy Center

*Audience: HR representatives*

*Assumptions: HR representative has printed the new employee's organizational information sheet and has a copy of the level to mandatory training matrix. The new employee is in orientation and has not started working full time. These procedures need to be carried out at promotion time and during the month of December for every employee to ensure that the correct modules are specified for the annual training period restart.*

### Business Justification:

In order to ensure that all employees who perform work for GIACENT receive the proper training, this process must be in place initiate this process. Moreover, this process provides the ability to record and track accountability and training module completion. This process also allows for verification for each employee and acts as an acceptance on the part of everyone at GIACENT of the overarching policy and underlying procedures implemented to protect the well being of the agency. In addition, in order to specify which training modules are administered and require completion for particular levels within GIACENT, their roles need to be matched with the threats that might be presented, and thus the appropriate training to circumvent those threats.

### Procedure:

1. Logon to secure training website, found in the HR web space
  - a. Access the intranet training website using a web browser at <https://www-i.hr.giacent.gov/training/admin>
  - b. Enter your administrator login name, pin number, and token in the appropriate fields and click on the **LOGIN** button.
2. Select the **Setup New Employee Program** from the available links
  - a. With the mouse, single, left click on the link
3. Choose the new employee and provide the necessary information
  - a. From the drop down box on the left, entitled **Employee Name**, select the correct Last, First name combination.
  - b. From the drop down box on the right, entitled **Manager's Name**, select the correct, corresponding Last, First name combination per the employee's information sheet.
  - c. In the **Start Date** text box, enter the employees first day on the job, following orientation; click on the **Update** button.
  - d. The **Completion Date** text box will be defaulted to 2 months from the date entered in the Start Date field.

- e. As indicated on the level to mandatory training matrix, place a check in the box (by clicking on the empty box) beside each training module required for the new employee under the **Required Training Modules** section; after each entry, click on the **Update** button to the right of the training. (The Completion Date field will be updated for 2 month increments, depending on the number of training modules required – 2 months are allotted for each).
  - f. Under the notification section, select one of the four radio buttons:
    - Contact both new employee and enforcing manager (**default**)
    - Contact new employee only
    - Contact enforcing manager only
    - Do not contact
4. Review the entered information and then select the **Confirm** button from at the bottom of the page.
  5. Review the read-only information displayed on the screen and choose the **Submit** button if the information is correct or the **Edit** button if changes are required.
  6. A confirmation message is displayed indicating who received notification (if applicable);
  7. Select the **End Session** link if you are finished with the application or the **Continue** link if more new employees are to be entered; Continue will take you back to the main links page; either button will simultaneously print the confirmation screen.
  8. Once you have logged out of the system, pick up the printed copy of the training confirmation and place into the employees personnel folder in the HR filing cabinets.
  9. The HR team lead must verify, by selecting employees at random, and reviewing their personnel file in the HR department to see if the training confirmation page, indicated above is placed in the folder.
  10. To ensure compliance, a plan should be developed in accordance with hiring and employee start dates for random checks of personnel files. In addition, prior to annual review sessions (April/September), sweeping verification should be performed by the HR Team lead to ensure compliance.
  11. With the mandatory training matrix on hand, the HR team lead must verify that the HR representatives are requiring the appropriate training on the training confirmation page from the Policy Center system.
  12. The HR Team Lead is required to present his/her findings at the monthly Security Advisory Board meeting following each verification session (randomly, May/October).
  13. *Note: The active HR representative is always carbon copied on all transactions performed in the Policy Center.*
  14. *Note: The director of HR should input all HR representatives' training submissions and is responsible for managing and enforcing their completion. The Security Advisory Board monitors all executives' training completion.*
  15. *Note: The Security Advisory board is exempt from the training because of their direct role in its creation and development; their familiarity with all of the subject matter should be sufficient.*

## Procedure for employee to execute training and learning assessment module

*Audience: All employees*

*Assumption: New employee has completed orientation and has received instructions and credentials regarding training awareness requirements. New employee has read and signed all acceptable use policies and email policy.*

### Business Justification:

To allow all GIACENT employees to receive and complete the proper training, this process must be in place to allow access to and record the employee's progress. This process automates training efforts and allows employees to work at their own pace and on their own schedules. This procedure also provides verification for each employee and allows for understanding and acceptance of the policies and procedures governing employee actions. Moreover, this procedure provides assessment for competitive and administrative purposes. Finally, and potentially most importantly, this procedure evaluates the effectiveness of the training modules by scoring the employees responses in a training assessment module. This provides a self check on the actual training material to ensure that it is clear, logical and understood by the GIACENT employees.

1. Logon to secure training website, found in the HR web space.  
*This step is required to gain logged access to the Web-based Policy Center application. You should have received a handout in your orientation material instructing you to login to the system for training and awareness requirements. Please see your HR representative if you do not have this information.*
  - a. Access the intranet training website using a web browser at <https://www-i.hr.giacent.gov/training>
  - b. Enter your login name, pin number, and token in the appropriate fields and click on the **LOGIN** button. (These credentials should be in your orientation manual).
2. Select the first training course/module that is listed as being required for your level and role. The training modules should be done in order to allow you the maximum amount of time to complete them (2 months).
  - a. From the list of training course modules, single, left click on the first one (that has not already been passed) to begin the course material
  - b. Once a course has been completed and the learning assessment passed, there will be a label next to the link indicating that the employee "Passed"
3. Read all course material and note questions in the web form.
  - a. Read all of the material on the page and when finished, click the **Next** button to advance in the course.
  - b. Continue this trend until you reach the end of the course.
  - c. There are text boxes at the bottom of each page in which questions and comments can be placed and reviewed at a later time.
  - d. On the last page of the course material, click on the **Learning Assessment Module** if you are ready to begin the test.
4. Attempt the learning assessment module



- a. Answer the multiple-choice questions by selecting the radio button next to the correct response.
  - b. Click on the **Next question** button when you are finished with the current question.
  - c. You can monitor your progress as you go through the learning assessment by looking at the progress bar at the bottom of the screen. To the right of the progress bar, it will have the number of the question you are attempting out of the total number of questions.
  - d. Your responses will be saved each time you click on the **Next** button, so that you can stop and restart when it is convenient for you to do so.
  - e. You can cycle through the questions using the **Next** and **Previous** buttons on either side of the progress bar.
  - f. Once you reach the final question; for example: **#30 out of 30** the **Next** button will be replaced with a **Submit** button.
  - g. Click on the **Submit** button and your responses will be graded and your results displayed with your confirmation of completion.
  - h. These results will be emailed to you, your manager, your HR representative and a copy will also be sent to your default printer.
5. Log out of the system by clicking the **End Session** button at the bottom of the screen.
  6. Pick up and turn in printed copy of training assessment results
    - a. Pick up printed training assessment results for module.
    - b. Sign agreement stating your compliance and authorization of the document.
    - c. Turn in signed results to your HR representative.
  7. Repeat these steps for each module that is listed under your required training modules after logging on to the training system again.
  8. Once you have completed all of the training modules you will have a label next to each of your required training modules indicating that you have completed that training module or not.
  9. All training modules must be completed. See Procedure #4: "Procedure for employee training module extension" if required.
  10. Each month, HR representatives should compile a list, by team, of completed and outstanding training requirements, based on their training submission records and emails sent to them by the Policy Center application, upon module completion by employees (see above). This report will outline who has and who has not completed their required training and if a majority of a team has not completed the required training, team leads should send a memorandum to each outstanding employee and submit his/her report (in the format below) to the Security Advisory Board as an issue at their monthly meeting.
  11. By every March 15<sup>th</sup> or 2.5 months following an employee's start date, Team leads should check personnel files to verify training completion against reports delivered by HR representatives. This is accomplished by requesting these documents from HR by filling out a request for training verification form (found in HR) or by physically going to HR's filing cabinets with an HR representative and pulling out the file and manually verifying the documentation. Discrepancies in HR representative's report findings and actual findings by team leads should be reported to the HR team lead and be submitted to the Security Advisory Board as an issue at their monthly meeting.
  12. Every April 10<sup>th</sup> and September 10<sup>th</sup> a report must be compiled and turned in to the Security Advisory Board by each team lead verifying who has and has not completed training. This document should be in Microsoft Excel format and should contain the following fields:

Name	Module	Completed (y/n)?	Score	Date	Level
------	--------	------------------	-------	------	-------

All non-completes should be highlighted by the use of red ink.

13. Based on this report, Advisory Board members should follow Procedure #5: "Procedure for disciplinary action for module non-completion" in reprimanding, depending on the level of delinquency, the employee.

© SANS Institute 2000 - 2002, Author retains full rights.

## Bibliography

McLeod, David. "LIONS and TIGERS and LAYERS (of security)." GIAC Information Officer Practical Assignment v.1.0. David\_McLeod\_GISO.doc. December 27, 2001. [0]

RSA Security, Inc. "Product information on RSA SecurID, RSA Keon Desktop, RSA Certificate of Authority". URL: <http://www.rsasecurity.com/products/>. (April 17, 2002). [1]

Internet Security Systems, Inc. "Product information on Managed Security Services". URL: [http://www.iss.net/securing\\_e-business/sec\\_management\\_sol/managed\\_sec\\_serv/](http://www.iss.net/securing_e-business/sec_management_sol/managed_sec_serv/). (April 17, 2002). [2]

Rozenblum, Danny. **Understanding Intrusion Detection Systems**. SANS Reading Room. August 9, 2001 [3]

IBM Corporation, The. "Research History Highlights" 1945 - 1996 URL: [http://www.research.ibm.com/about/past\\_history.shtml](http://www.research.ibm.com/about/past_history.shtml) (April 17, 2002) [4]

Lemos, Robert. "Mitnick Teaches Social Engineering." July 16, 2000. URL: <http://zdnet.com.com/2100-11-522261.html?legacy=zdn> (April 17, 2002). [5]

Pentasec Security Technologies, Inc. "Product information on VigilEnt Policy Center". URL: <http://www.pentasec.com/products/>. (April 17, 2002). [6]

Tims, Rick. **Social Engineering: Policies and Education a Must**. February 16, 2001. URL: <http://rr.sans.org/social/policies.php> (April 17, 2002). [7]

Smith, Sandi. "The Risks and Rewards of Information Security Planning." December 19, 2000. URL: <http://www.toptentechs.com/issues/Issue1/> (April 17, 2002). [8]

Palumbo, John. **Social Engineering: What is it, why is so little said about it and what can be done?** SANS Reading Room. July 26, 2000. (April 17, 2002). [9]

Symantec, Inc. "Product information on desktop anti-virus corporate edition and Symantec Security Services". URL: <http://www.symantec.com/product/> (April 17, 2002). [10]

Baldwin, Michael. "Security breach blamed on janitor." August 2001. URL: <http://www.yrnews.com/archives/baldwin.htm> (April 17, 2002). [11]

Lemos, Robert. "A year later, dDoS attacks still a major Web threat." February 07, 2001. URL: <http://news.com.com/2009-1001-252187.html?legacy=cnet> (April 17, 2002). [12]

Nokia Fireguard HA + 540 Firewall Product. & Nokia Firewall/VPN Product URL: [http://www.nokia.com/securenetworksolutions/itcm/server\\_appliances.html](http://www.nokia.com/securenetworksolutions/itcm/server_appliances.html) & [http://www.nokia.com/vpn/firewall\\_vpn.html](http://www.nokia.com/vpn/firewall_vpn.html) . [13]

Shipley, Greg. "Anatomy of a Network Intrusion." October 18, 1999. URL: <http://www.networkcomputing.com/1021/1021ws1.html> (April 17, 2002). [14]

Security Focus Online. "Vulnerabilities." Current. URL: <http://www.securityfocus.com/cgi-bin/vulns.pl> (April 17, 2002). [15]

Associated Press. "Computer Attacks on the Rise, says FBI study." April 08, 2002. URL: [http://timesofindia.indiatimes.com/articleshow.asp?art\\_id=6290056](http://timesofindia.indiatimes.com/articleshow.asp?art_id=6290056) (April 17, 2002). [16]

Beaver, Kevin. "The 21 best ways to lose your information." April 12, 2002. URL: [http://www.computerworld.com/cwi/community/story/0,3201,NAV65-663\\_STO70076,00.html](http://www.computerworld.com/cwi/community/story/0,3201,NAV65-663_STO70076,00.html) (April 17, 2002). [17]

National Security Agency. "Security Recommendation Guides" March 06, 20002. URL: <http://nsa1.www.conxion.com/win2k/download.htm> (April 17, 2002). [18]

SANS Institute, The. "Certified Information Security Officer Training" Track 9: Defense in Depth (March 2002): pp 1-67. [19]

SANS Institute, The. "Certified Information Security Officer Training" Track 9: Proven Practices for Managing the Security Function (March 2002): pp 97-125. [20]

Voss, Brian D. **The Ultimate Defense of Depth: Security Awareness in Your Company.** SANS Reading Room. August 11, 2001. [21]

Forristal, Jeff. Shipley, Greg. "Vulnerability Assessment Scanners" January 8, 2001. URL: <http://www.networkcomputing.com/1201/1201f1b3.html>. (April 17, 2002). [22]

Zarate, Raul. "Securing your network perimeter". SANS Reading Room. April 4, 2001. URL: [http://www.sans.org/infosecFAQ/audit/net\\_border.htm](http://www.sans.org/infosecFAQ/audit/net_border.htm). (April 17, 2002). [23]

CISCO 12000 Border Router. URL: <http://www.cisco.com/warp/public/cc/pd/rt/12000/> (April 17, 2002). [24]

Buonocore, Kathleen. **Selecting an Intrusion Detection System.** SANS Reading Room. August 19, 2001. [25]

Nokia Corporation . " Nokia / Internet Security Systems partnership delivers intrusion detection breakthrough." May 09, 2000. URL: [http://press.nokia.com/PR/200005/780695\\_5.html](http://press.nokia.com/PR/200005/780695_5.html) (April 17, 2002). [26]

Tiny Personal Firewall 2.0.5A. 2002. URL: <http://www.tinysoftware.com> (April 17, 2002). [27]

PGP Freeware 7.0.1. 2002. URL: <http://www.pgp.com>. (April 17, 2002). [28]

Brewer, David. "Easy ways to manage your risk". Gamma Secure Systems Limited. URL: <http://www.gammasl.co.uk/topics/hot10.html> (April 17, 2002). [29]

Farmer, Dan & Venema, Wietse. "Improving the Security of your Site by Breaking into it." URL: <http://www.fish.com/security/admin-guide-to-cracking.html> (April 17, 2002). [30]

SANS Institute, The. "'Internet Storm Center" URL: <http://www.incidents.org/> (April 17, 2002). [31]

CERT. URL: <http://www.cert.org/>. (April 17, 2002). [32]

Crunch, InstallWrap, Softlocx. 2002. URL: <http://www.bit-arts.com/> (April 17, 2002). [33]

International Biometric Group. Retina product. 2002. URL: <http://www.biometricgroup.com/> (April 17, 2002). [34].

NSA Information type guide. Actually developed for client; adapted for GIACENT's purposes. [35]

SonicWall Pro 300. Hardware firewall solution. URL: [http://www.tribecaexpress.com/sonicwall\\_firewalls.htm](http://www.tribecaexpress.com/sonicwall_firewalls.htm) (April 17, 2002). [36].

Nortel Networks Extranet Client. 2002. URL: <http://www.nortelnetworks.com/> (April 17, 2002). [37].

NIST. Guide for Developing Security Plans for Information Technology Systems, December 1998. URL: <http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc> (April 17, 2002). [38]

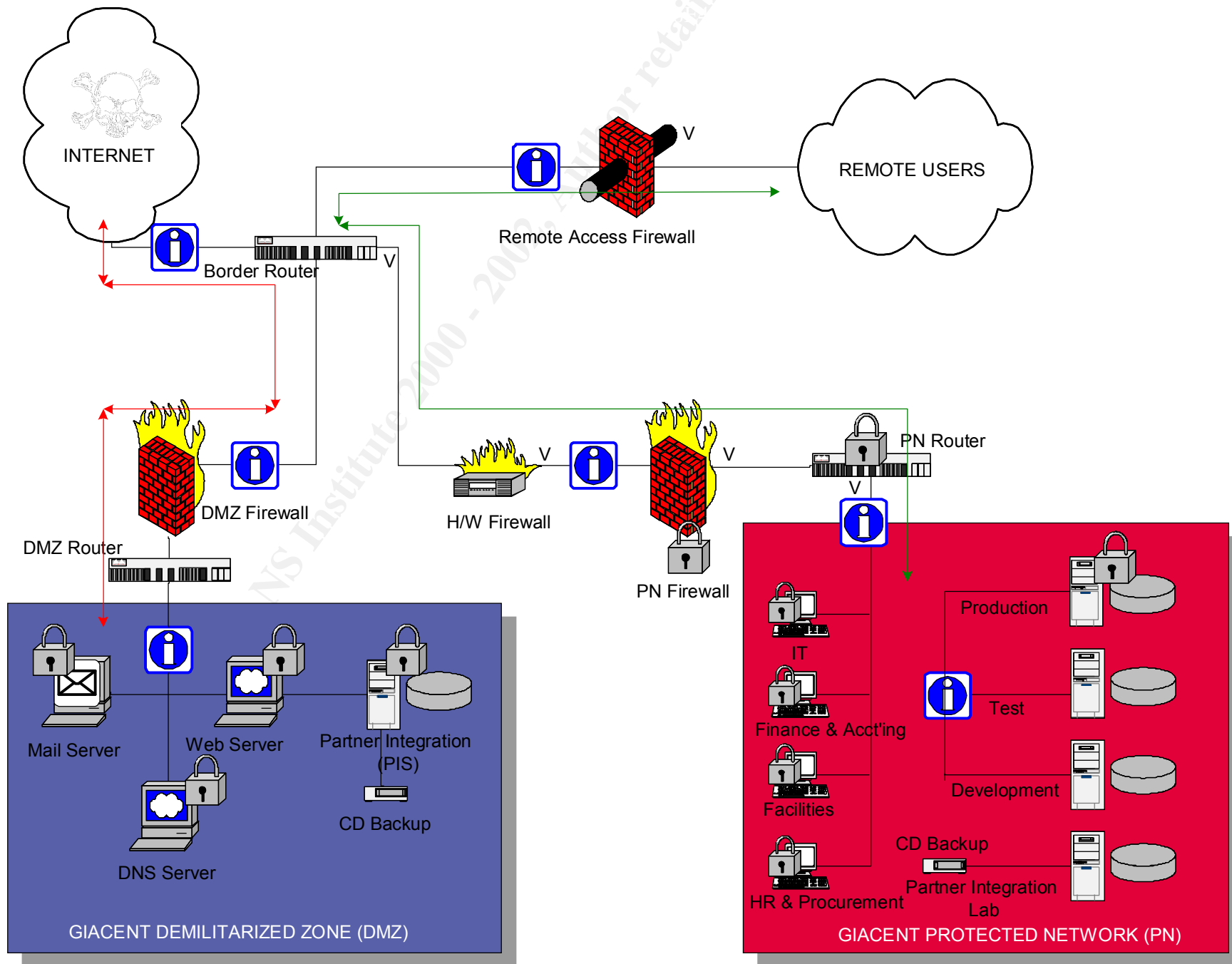
Additional information and graphics were borrowed from my professional work and experience in the areas of risk assessment and security architecture.

© SANS Institute 2000 - 2002, Author retains full rights.

## APPENDIX

© SANS Institute 2000 - 2002, Author retains full rights.

Figure 1: GIACENT Network Topology



**Figure 2: GIACENT Security Information Classification**

Information Type	Confidentiality	Integrity	Availability
SOE Source Code	H	H	H
Application Source	H	H	H
Financial	H	M	M
Human resources	M	M	L
Non-sensitive information	L	L	L
Sensitive information	H	H	L
Non-GIACENT data	H	H	M
Public GIACENT documentation	L	M	L
Facility Drawings	M	M	M
Mailing List	L	L	L
Security/ Safety Alerts	L	M	H
Backups	H	H	H

**Definitions of Sensitivity:** *Confidentiality* – The system contains information that requires protection from unauthorized disclosure. *Integrity* – The system contains information which must be protected from unauthorized, unanticipated, or unintentional modification. *Availability* - The system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses. <sup>[38]</sup>

**Definitions of Criticality Levels:** *High* — a critical concern of the system; *Medium*— an important concern, but not necessarily paramount in the organization's priorities; or *Low* — some minimal level of security is required, but not to the same degree as the previous two categories. <sup>[38]</sup>

**Figure 3: GIACENT Asset Details**

Machine	OS(s)	Apps	Hardware	Administrator
Mail Server	RedHat Linux 7.2	sendmail, ISS RealSecure Server 6.0.1, Tripwire 2.4.2	Compaq ProLiant DL580 1.2Ghz Xeon, 1.5GB RAM	Operational Security
DNS Server	RedHat Linux 7.2	BIND, ISS RealSecure Server 6.0.1, Tripwire 2.4.2	Compaq ProLiant DL580 850Mhz Xeon, 924MB RAM	Operational Security



Web Server	Sun Solaris 8	iPlanet Webserver 4.0, ISS RealSecure Server 6.0.1, Tripwire 2.4.2	Compaq ProLiant DL580 1.5Ghz Xeon, 2GB RAM	Operational Security
PIS	SOE	GIACENT Environment Integration Testing App, Windows 2000 Authenticator module, ISS RealSecure Server 6.0.1	Compaq ProLiant DL580 1.8Ghz Xeon, 2GB RAM, Kenwood 72X Cdrom drive	Operational Security
IT Department	MIX; Servers: Windows 2000 Advanced Server, RedHat Linux, Sun Solaris; Routers/Switches: IOS Workstations: Windows 2000	Varies: Microsoft Office 2000 Suite, Symantec Antivirus, Tiny Personal Firewall, PGP Freeware 7.0.1, Asset management software; ISS RealSecure Server Sensor 5.0, Tripwire 2.4.2	User desktops: Compaq ProLiant DL380 1Ghz Pentium III, 1GB RAM Windows 2000 SP2	Information Technology
F & A Department	Windows 2000	SAP-ERP; Asset management, ISS RealSecure Server Sensor 5.0	HP-UX 10.0.1 EMC Symmetrix 8830 1TB SAN Storage	Information Technology
Facilities Department	Windows 2000	SAP-ERP; Asset management, ISS RealSecure Server Sensor 5.0	HP-UX 10.0.1 EMC Symmetrix 8830 1TB SAN Storage	Information Technology
HR & Procurement Department	Windows 2000	SAP-ERP; Asset management, ISS RealSecure Server Sensor 5.0	HP-UX 10.0.1 EMC Symmetrix 8830 1TB SAN Storage	Information Technology
Production Environment	SOE	ISS RealSecure Server 6.0.1, Tripwire 2.4.2	Compaq ProLiant DL880 4x2Ghz Titanium, 4GB RAM	IT, Op Sec, Development
Test Environment	SOE, MIX	TestRunner Test Pro	Compaq ProLiant DL880 4x1Ghz Titanium, 2GB RAM	IT, Op Sec, Development
Development Environment	SOE, MIX	Development Tools	Compaq ProLiant DL880 2x1Ghz Titanium, 1GB RAM	IT, Op Sec, Development
PIS Laboratory (5)	SOE, MIX	Development Tools	Compaq ProLiant DL580 2x1Ghz Xeon, 1.25GB RAM, Kenwood 72X Cdrom drive	IT, Op Sec, Development
Routers/Switches	IOS	Tripwire 2.4.2	Cisco / ISA VPN adapter	IT, Op Sec, Development
*MIX - this department has a combination of machines consisting of Windows 2000, Linux, Solaris 8, IOS and HP-UX, in order of quantity				
GIACENT Environment Integration Testing App is responsible for accepting packaged files from authenticated users, unpackaging, installing, running and reporting the results of the program execution to the Web Server in the DMZ.				