# Global Information Assurance Certification Paper

# GIAC SECURITY LEADERSHIP CERTIFICATE

# PRACTICAL ASSIGNMENT



**DOMINIC A. NESSI, CISSP**
**AUGUST 13, 2003**
**VERSION 1.0**

## ABSTRACT

Federal Agencies face numerous problems in today's IT environment in the area of security. Mitigation of these issues is significantly hampered by a lack of funding, competing demands and lack of understanding of security issues by management and employees alike. Three questions are the focus of this paper: 1) What elements in the federal IT culture resulted in a lack of attention to IT security by federal domestic agencies; 2) Why did it take Congressional mandates to spur federal agencies to action; and 3) Now that IT security issues have become of paramount importance, what can federal agencies do to meet the challenge?

In answer to the final question, this paper offers ten important security measures that can be accomplished without cost or at a low cost.

## IMPORTANCE OF THIS TOPIC

This topic is of critical importance for federal agencies and IT professional managers such as Chief Information Officers, especially in today's IT environment. IT security is the subject of critical federal legislation, the Office of Management and Budget (OMB) regulations and Congressional oversight. In light of the importance of this effort, it is ironic that neither Congress nor OMB has funded IT security at a level consistent with the attention that it requires. Agency management attention to program priorities more often than not follows where the Congress allocates funding. As a result, top management rarely focuses on IT security and CIOs and agency IT staff are left to find inexpensive solutions to mitigate security issues.

Finding low-cost and effective solutions is essential. Using a checklist approach to IT security provides a low-cost method for ensuring that most basic security measures have been addressed. This paper provides a ten point checklist that can be used by federal managers, as well as CIOs and other IT professionals in a leadership role.

## INTRODUCTION

Most federal agencies have only recently begun to come to grips with the security of their information systems and information technology (IT) infrastructure. Despite a series of statutes, beginning in 1987 with the Computer Privacy Act, and Office of Management and Budget (OMB) guidance, such as OMB Circular A-130, Appendix III few agencies considered IT security to be anything more than an additional operational requirement.

However, in the past two or three years, IT security awareness among federal agencies has been spurred by two distinct influences. First, the number of worms, viruses and hacker attempts that pervading the Internet has grown dramatically. In 1990, estimates ranged from 200 to 500; then in 1991 estimates ranged from 600 to 1,000 different viruses. In late 1992, estimates were ranging

from 1,000 to 2,300 viruses. In mid 1994, the numbers vary from 4,500 to over 7,500 viruses. In 1996 the number climbed over 10,000. 1998 saw 20,000 and 2000 topped 50,000. [1]

The second is the external pressured applied by the Congress with the annual publication of the "Horn Report". Beginning in 1999, former Congressman Stephen Horn, from California, from his position as Chairman of the House Government Management, Information and Technology Subcommittee, began publishing an annual report on the state of IT security at federal agencies. In the latest report, dated November 14, 2002, 14 of the 24 federal agencies graded received a grade of "F". [2]

The result of the Horn Reports and other publicized security breaches spurred the passage of two key legislative initiatives. The first was the Government Information Security Reform Act (GISRA) which was enacted in 2000.[3] The emphasis of the GISRA Security Act lies in:

- Full asset life cycle security
- management procedures
- Incident Response Capability
- Annual Program Review
- Deficiency Reporting
- Annual Performance Plans

The second Act follows up on GISRA and is the Federal Information Security Management Act of 2002 (FISMA) which ensures the effectiveness of information security controls over information resources that support Federal operations and assets.

Three questions are the focus of this paper: 1) What elements in the federal IT culture resulted in a lack of attention to IT security by federal domestic agencies; 2) Why did it take Congressional mandates to spur federal agencies to action; and 3) Now that IT security issues have become of paramount importance, what can federal agencies do to meet the challenge?

*Lack of Attention to IT Security by Federal Agencies*

Like the private sector, the past two decades have seen an explosive change in the federal computing environment with a staggering increase in the use of personal computers (one on every desk), interconnectivity using local area networks (LANs), metropolitan area networks (MANs) and wide area networks

[1] C-Systems Virus Tutorial, www3.sk.sympatico.ca
[2] Federal Computer Week, December 2, 2002. "Horn: Feds Still Fail Security. Horn's third 'report card' finds little improvement"
[3] Federal Computer Week, March 28, 2003. "Government's Security Advantage"

(WANs), and, finally, access to the Internet. Government IT infrastructures were built for open computing and public accessibility was an extremely important component in web development.

Application management is widely dispersed amongst the literally thousands of federal program administrators with little centralized professional IT management and oversight. With an increase of telecommuting, as well as employees using their work PCs for limited personal use, each desktop becomes a potential source for an external threat. In fact, federal employees not only desire, they have grown to expect significant freedom in how they use their own desktop computing devices, wireless PDAs, cell phones, and other technology devices.

Finally, federal agencies have simply not been funded to perform either the necessary planning which is essential to ensure that security measures are properly designed or to acquire the security improvements themselves. Some federal officials, such as Mark Forman, former associate director of IT and e-government at the Office of Management and Budget, attribute the problem to the fact that "many agencies are not adequately prioritizing their IT investments." They ask for money to develop new systems but have largely failed to improve the security of those they already operate, Mr. Forman has said.[4]

Unfortunately, this criticism misses the obvious. As long as Congress continues to enact new legislation creating new programs and/or asking for information on existing programs, federal agencies must and will continue to develop new applications. There is simply no choice.

These environmental components coupled with the fact that federal agencies themselves do not suffer harm from improper release or loss of data (as opposed to a business who can be sued, lose a competitive edge or simply go out of business) has made IT security a low priority for non-IT program managers.

*Why Did It Take a Congressional Mandate for Agencies to Act?*

Federal agencies have so many demands on limited budgets these days that it is impossible to meet every possible requirement. Federal managers have little choice but to pay attention to the “squeakiest” wheels. IT security traditionally finished low on the priority list because IT security breaches were focused such concerns as an occasional shutdown due to a rampaging virus, web defacements from disgruntled groups, sporadic releases of personal or confidential information, and the internal employee manipulating applications for their own personal gain. As important as these threats are to IT professionals, non-IT managers typically saw these issues as something the IT “guys” will just need to stay a little later and “fix the problem” so the organization can get up and running again.

[4] Federal Computer Week, December 2, 2002. “Horn: Feds Still Fail Security. Horn's third 'report card' finds little improvement”

Funding, or the lack of it, prohibits federal agencies from embracing a comprehensive IT security program because it comes at the expense of other priorities. Even the federal budget cycle which literally begins at the agency level two years before an actual fiscal year commences, is an obstacle for agencies which have the desire to take an aggressive security approach.

Despite the passage of GISRA, concern remained low until September 11, when it became clear to all Americans that terrorism can occur and come in many forms and that many of federal systems had potentially critical information that could be used against us as well as the potential damage from simply shutting down our IT infrastructure. The world changed permanently for federal IT professionals after that tragic event.

*What Can Federal IT Managers Do to Meet the Challenge?*

How does a federal manager, IT or program manager, balance these seemingly diametrically opposed influences? We have systems developed for open access in a world where open access is becoming increasingly dangerous. We have limited funds for IT security improvements and continued pressure for new applications to meet business needs. Federal managers and employees, for the most part, do not see any potential damage as a result of IT security breaches and take the position that "security goes unfixed until it is proven that it is broken."

Despite these obstacles, there are ten things a federal IT manager can do to substantially increase IT security immediately and without significant new funding. They are listed below in no particular order, but all are equally important.

**IT Security Awareness Training** – IT security training should be created for three specific groups: 1) IT specialists, program managers; and 3) the entire employee population. Training should be tailored to the needs of each and can be very inexpensive. Numerous federal agencies offer training courses, such as the Defense Information Systems Agency (DISA), which can be had for no charge and modified to fit the specifics of an individual agency. IT security begins with awareness at all levels of the organization and regular training and reinforcement of IT security principles is essential to change the mind-set currently pervasive in the federal sector.

**Password Policies -** Passwords are an important aspect of computer security and the front line of protection for user accounts. And the best thing about implementing a strong password policy is that is free. It is important that employees learn through their IT security awareness training that a poorly chosen password may result in the compromise of an agency's entire corporate network. They must learn that "it can happen to them". There are numerous sample password policies that can be used, including one developed by SANS. Most federal agencies use the guidance set by the National Institute of Standards and Technology (NIST) in NIST 800-14 and enhanced by industry best practices.

The best passwords have lengths greater than eight characters, use numbers, letters, and special characters in both upper and lower case. Passwords should not be obvious such as names, places or something that can be connected to the user. The best passwords have no meaning at all.

**Incident Response** – Even the most expensive security and prevention tools fail. Thus, it is critical for agencies to be ready to respond when an incident occurs such as viruses, malicious user activity, etc. Such incidences require a skilled and rapid response before they can cause significant damage. NIST 800-3 offers a series of actions a federal agency can take that are low in cost, but critical in time of an emergency. NIST describes these efforts as Computer Security Incident Response Capabilities (CSIRCs).[5]

CSIRCs have as a primary focus the goal of reacting quickly and efficiently to computer security incidents. CSIRC efforts provide agencies with a centralized and cost-effective approach to handling computer security incidents so that future problems can be efficiently resolved and prevented. CSIRC is a direct extension of the contingency planning process, due to its explicit preparedness to respond to threats as they occur.

A CSIRC is best established as a central capability for dealing with virtually any computer security problem that occurs. It provide a means for reporting incidents and for disseminating important incident-related information to management and users. It should concentrate the coordination of incident handling into one effort, thereby eliminating duplication of effort.

CSIRC is based on policies and guidance and communication.

**Intrusion Detection** – There are numerous intrusion detection systems (IDS) that agencies can employ, again some of the being very inexpensive and in some cases free, such as SNORT which is an open source intrusion detection system. Intrusion detection systems work in two primary ways. First, IDS detects intrusions by looking for activity that is different from a user's or system's normal behavior. Second, IDS detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities.

Many intrusion detection systems base their operations on analysis of audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

An IDS may also perform its own system monitoring. It may keep aggregate statistics which give a system usage profile. These statistics can be derived from

[5] **NIST SPEC PUB 800-3** ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC) By John Wack November 1991

a variety of sources such as CPU usage, disk I/O, memory usage, activities by users, number of attempted logins, etc. These statistics must be continually updated to reflect the current system state.

They are correlated with an internal model which will allow the IDS to determine if a series of actions constitute a potential intrusion. This model may describe a set of intrusion scenarios or possibly encode the profile of a clean system.

IDS is an important and cost-effective source for federal agencies to gain intelligence on what type of random or targeted threats are being aimed at them.

**Perimeter Security –** Perimeter security is essential. Typically an agency's intranet should be a self-contained infrastructure with limited access to the outside world. The only entry points or gateways should be with Internet points-of-presence or POPs or where an agency has remote offices that require the use of local Internet service providers (ISPs) for their access.

When a network infrastructures is clearly delineated, documented and defined, the agency can protects its "borders" through the development of strict policies and the gateways. The key is documentation and a strong policy coupled with compliance measures that prohibits users from adding entry points without a careful decision as to the impact on security.

**Simple Firewalls** – Though firewalls can be very expensive, even a low-cost firewall provides an enhanced level of protection if managed properly by acting as the first line of defense in preventing improper access into the network and servers from unauthorized parties. In fact, a few well-placed firewalls within the network can severely limit the internal threat from malicious employees who are either seeking to damage valuable data assets, release confidential information or misappropriate funds through manipulation of financial systems.

Firewalls come from a variety of vendors and range from simple to quite complex. However, even the most financially stressed federal agency can afford some level of firewall protection

**DMZs –** Any federal agency that has public-facing web servers should create a perimeter security network called a demilitarized zone (DMZ) that separates the internal network from the outside world.

DMZs are the best place for publicly accessible information for the public, partners, customers to obtain the information that they need without accessing the agency's internal network. Sensitive and confidential should be stored behind the DMZ on the internal network. As a result, a breach of the DMZ servers should at worst create an annoyance in the form of downtime during the recovery from the security breach.

Typical systems that are found in a DMZ are as follows:

- A Web server that holds public information.

- The front end to an e-government transaction server through which the public submits information.
- A mail server that relays outside mail to the inside.
- Authentication services and servers that let access into the internal net.
- VPN endpoints.
- Application gateways.
- Test and staging servers.

Typically services like HTTP for general public usage, secure SMTP, secure FTP, and secure Telnet are deployed on the DMZ.

To build a DMZ, the agency's firewall has to have three network interfaces, as most already do at present. One interface goes to the inside of the network, one goes to the un-trusted Internet, and the third goes to the DMZ. The DMZ consists of those servers needed to connect outside of the firewall. Servers containing mission critical data are protected behind the firewall.

The firewall is configured to put tight restrictions on the traffic that is let through to the internal network, and use different, and perhaps less restrictive rules for the DMZ. For example, the agency can allow HTTP to the Web-server on the DMZ, but not allow HTTP to the internal network. Systems in the DMZ should be as securely locked down as possible in order to prevent unauthorized behavior on the DMZ itself. The agency can monitor machines on the DMZ fairly simply, because it knows what ports need to be used, and how the general public or internal employees need to make use of the DMZ servers.

**Patch Management –** Though patch management products do have a cost, they are a critical element of network infrastructure management. A patch management product automatically detects security vulnerabilities on the network by checking for all potential methods that a hacker might use to attack it. By analyzing the operating system and the applications running on a network, it identifies possible security holes. In other words, it plays the devil's advocate and provides an alert to weaknesses before a hacker can find them, enabling the organization to deal with these issues before a hacker can exploit them.

Typically, a patch management product scans the entire network, IP by IP, and provides information such as service pack level of the machine, missing security patches, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups, and more. Scan results are outputted to an HTML report, which can be customized/queried, enabling the agency to proactively secure its network - for example, by shutting down unnecessary ports, closing shares, installing service packs and hot fixes, etc.

**Antivirus Software** – Antivirus software is a program that looks for known viruses by checking for recognizable patterns checks for viruses while other

programs are running. They are fairly inexpensive, some such as InoculateITPE from Computer Associates are free, and critical to ensure protection against the growing number of worms and viruses. An enterprise agreement is essential for all federal agencies. First it ensures that all equipment is protected. Second, it allows for updates to the software as new virus patterns are discovered.

NIST recommends using a two-tiered approach for detecting and preventing viruses from spreading:

- On personal computers, install and use anti-virus software capable of scanning disks, attachments to email, files downloaded from the web, and documents generated by word processing and spreadsheet programs.
- Use anti-virus software at Internet gateways or firewalls to scan email attachments and other downloaded files.

**Background Checks** - Any time an IT candidate is about to be hired as either a federal employee or a contractor, a federal agency is required to do at least a basic background check depending on the level of sensitivity of the system. Yet despite the requirement, few agencies actually ensure the checks are carried out and other agencies reduce the level of sensitivity of their systems in order to require lesser checks. Background checks are essential and should begin with a thorough review of the resume. Frequently, if information is incorrect or inaccurate on the resume, there is the potential that additional issues may result from a more thorough background check.

More thorough background checks on non-IT employees with ancillary IT duties, such as timekeepers, administrative assistance, financial analysts and accounting technicians are equally critical. IT security threats from with in represent the largest total threat and too many agencies believe that their employees are “too loyal” to ever commit an unacceptable act. They are often proven wrong and they find in retrospect that the first indication of a problem could have been found by a more thorough review before the employee was hired.

**Bonus Checklist Item – Hire a Security Specialist.** It is essential that an agency have at least one person who is a specialist in IT Security. That person must have autonomy from IT operations and have the freedom to call into question IT procedures and practices that do not meet an adequate level of IT security. The higher in the IT organization that the security specialist’s position resides, the more influence they will have in the eyes of management, users and other program officials. The IT security specialist should be well trained and conversant in IT security measures.

References

**E-Business Special report:** IT Security on a Shoestring Budget. By Tiernan Ray E-Commerce Times. March 17, 2003

National Institute of Technology Standards – **NIST SPEC PUB 800-12**
AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK

**NIST SPEC PUB 800-18**
GUIDE FOR DEVELOPING SECURITY PLANS FOR INFORMATION TECHNOLOGY SYSTEMS

**NIST SPEC PUB 800-14** GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURING INFORMATION TECHNOLOGY SYSTEMS

**NIST SPEC PUB 800-3**
ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

SANS Security Essentials with CISSP CBK Version 2.1. Volume One and Two

Inside Network Perimeter Security. Stephen Northcutt, Lenny Zelster, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey

Information Security Management Handbook 4th Edition. Harold F. Tipton, Micki Krause

Information Security Architecture: An Integrated Approach to Security in the Organization. Jan Killmeyer Tudor

Last Updated: July 27th, 2017

# Upcoming Training


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