Global Information Assurance Certification Paper

Federal Systems Level Guidance for Securing Information Systems

By

James Corrie

GSEC Practical Assignment Version1.2e

August 16, 2001

TABLE of CONTENTS

Introduction:

A global explosion of Internet connected information systems has taken place over the past several years. It is estimated that over 90 million computer systems are currently deployed worldwide. With this rapid increase of system deployment the information security community has witnessed a dramatic increase in the number of private, business and government networks being compromised. The threat of information systems succumbing to vulnerabilities is increasing with the number of systems deployed. In recent months The SANS Institute's Internet Storm Center has detected coordinated international and domestic attacks directed specifically at United States information systems. Some international attacks have been quite successful against international and domestic systems; some attacks have not (can anyone say "l1on" and "Red Worm"?). A Congressional oversight committee has learned that despite strenuous efforts by the U.S. Government, more than 155 separate Government computer systems were temporarily taken over by hackers last year. The need for security guidelines and defense-in-depth strategies has never been greater. As a result Federal legislation has been / is being enacted to aid in securing of national information systems. The United States Federal Government has mandated government-wide information technology security reform and accountability. Several governmental agencies have developed system level guidelines for securing system implementation, system hardening, and system disposal at the end of its life cycle. These guidelines can apply to both the governmental and private sector.

Legislation:

For the Federal government it is more important than ever to have security policy, "locked down" information systems, assessment testing and documentation of the results. A myriad of new and revised Federal guidelines are in effect. These mandates are designed to tie information security; system management and budget together and as a result promote a stronger, more secure government information technology infrastructure.

The driving force behind this information technology reform is the Computer Security Act of 1987: PL 100-235. The Computer Security Act has a dual purpose. First, it improves the security and privacy of sensitive information in Federal computer systems and establishes minimal security practices. Secondly, the Computer Security Act assigns the National Institute of Standards and Technology (NIST) the responsibility for developing standards and guidelines required to implement cost-effective security and privacy in Federal information systems with the advise / assistance of the National Security Agency (NSA). This act paved the way for protecting systems by codifying the security planning and training requirement for the US Government.

The Office of Management and Budget's (OMB) Circular No. A-130, Appendix III was amended on November 28, 2000 to reflect the incorporation of the requirements of the Computer Security Act of 1987 and include the responsibilities assigned in national security

directives. This appendix outlines the minimal security controls to be included in Federal information systems and assigns responsibilities for security of Federal information systems.

On October 30, 2000 the Government Information Security Act (GISRA) was signed into law and amended the Paperwork Reduction Act (PRA) of 1995. GISRA addresses the program management, implementation, and evaluation of information system security for classified and unclassified systems. This act also requires annual assessment of information systems by the sponsoring agency and an independent source. The Chief information Officer and Inspector General must jointly submit this report, along with the independent security assessment, to the Office of Management and Budget.

System Level Guidance for Government Agencies & Private Industry

Well now, we have all sorts of legislation that directs this and mandates that but what do all these regulations mean to the computer specialists and system administrators in the trenches? All the white paper can be overwhelming but how do we extract the vital information needed to implement security policy, "lock down" our operating systems, secure our system perimeters and make the appropriate changes to our existing IT infrastructure? How do we ensure the three basic elements of system security: confidentiality, integrity, and availability? Below you will find some agencies that have supplied information and the materials to take on this task.

The National Institute of Standards and Technology (NIST) History & Authority:

On March 3, 1901 the United States Department of Commerce's National Bureau of Standards was created. In 1988 the National Bureau of Standards was renamed the National Institute of Standards and Technology (NIST). NIST celebrates its 100th birthday this year. The current President, George Bush congratulated NIST on its birthday by stating, " As part of the United States Department of Commerce, the National Institute of Standards and Technology remains the steward of the United States measurement system and is known for its achievements in physical measurements, standards developments, test methods, and basic scientific and technical research."

In June 2001 National Institute of Standards and Technology's (NIST) Information Technology Laboratory (ITL) released NIST Special Publication (SP) 800-27, "Engineering Principles for Information Technology Security (EP-ITS)" to assist in the secure design, development, deployment and life-cycle of information systems. The audiences this document targets are: average users; system engineers and architects; program managers and information security officers. This document presents 33 security principles which start at the design phase of the information system / application and continue until the system's retirement / secure disposal. This is in accordance with the planning phases outlined in the NIST special publication, "Generally Accepted Principles and Practices for Securing Information Technology systems, SP 800-14. The phases are:

1. Initiation phase
2. Development /acquisition phase
3. Implementation phase

4. Operation/maintenance phase
5. Disposal phase

These NIST principles cover a defense-in-depth approach to security.

Table 1: EP-ITS Engineering Principles

Principle 1.	Establish a sound security policy as the "foundation" for design.
Principle 2.	Treat security as an integral part of the overall system design.
Principle 3.	Clearly delineate the physical and logical security boundaries governed by associated security policies.
Principle 4.	Reduce risk to an acceptable level.
Principle 5.	Assume that external systems are insecure.
Principle 6.	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
Principle 7.	Implement layered security (Ensure no single point of vulnerability.).
Principle 8.	Implement tailored system security measures to meet organizational security goals.
Principle 9.	Strive for simplicity.
Principle 10.	Design and operate an IT system to limit vulnerability and to be resilient in response.
Principle 11.	Minimize the system elements to be trusted.
Principle 12.	Implement security through a combination of measures distributed physically and logically.
Principle 13.	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
Principle 14.	Limit or contain vulnerabilities.
Principle 15.	Formulate security measures to address multiple overlapping information domains.
Principle 16.	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
Principle 17.	Use boundary mechanisms to separate computing systems and network infrastructures.
Principle 18.	Where possible, base security on open standards for portability and interoperability.
Principle 19.	Use common language in developing security requirements.
Principle 20.	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
Principle 21.	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Principle 22.	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
Principle 23.	Use unique identities to ensure accountability.
Principle 24.	Implement least privilege.
Principle 25.	Do not implement unnecessary security mechanisms.
Principle 26.	Protect information while being processed, in transit, and in storage.
Principle 27.	Strive for operational ease of use.
Principle 28.	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
Principle 29.	Consider custom products to achieve adequate security.
Principle 30.	Ensure proper security in the shutdown or disposal of a system.
Principle 31.	Protect against all likely classes of "attacks."
Principle 32.	Identify and prevent common errors and vulnerabilities.
Principle 33.	Ensure that developers are trained in how to develop secure software.

The chart presented below gives a cross reference of how the 33 engineering principle relate to information system life cycle phases.

Principle Applicability to System Life-Cycle Phase

The five life-cycle planning phases used are defined in NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*:

- Initiation Phase
- Development/Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase.

In an effort to associate each principle with the relevant life-cycle planning phase(s), Table 2 summarizes the relationship between the 33 principles and the life-cycle phases to which they apply. The table identifies each life-cycle phase, and "check marks" are used to indicate if the principle should be considered or applied during the specified phase. One check "✔" signifies the principle can be used to support the life-cycle phase, and two checks "✔✔" signifies the principle is key to successful completion of the life-cycle phase.

Who we are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

Table 2: Principle versus Life-Cycle Phases

	Life-Cycle Applicability				
Principle	**Initiation**	**Devel/Acquis**	**Implement**	**Oper/Maint**	**Disposal**
1	✔✔	✔	✔	✔	✔
2	✔✔	✔✔	✔✔	✔✔	✔
3	✔✔	✔✔	✔	✔	
4	✔✔	✔✔	✔✔	✔✔	✔✔
5	✔✔	✔✔	✔✔	✔✔	✔
6	✔✔	✔✔		✔✔	
7	✔	✔✔	✔	✔✔	✔
8	✔	✔✔	✔	✔✔	✔
9	✔	✔✔	✔	✔✔	
10	✔	✔✔		✔✔	
11	✔	✔✔	✔	✔✔	
12		✔✔	✔	✔	✔
13	✔	✔✔	✔	✔✔	✔
14		✔✔	✔	✔	
15	✔	✔✔	✔	✔	
16	✔	✔✔	✔	✔	
17		✔✔	✔	✔✔	
18	✔	✔✔	✔		
19	✔✔	✔✔		✔✔	
20	✔	✔✔	✔✔	✔	
21		✔✔	✔	✔✔	
22	✔	✔	✔	✔✔	
23	✔	✔	✔	✔✔	
24	✔	✔	✔	✔✔	
25	✔	✔✔	✔✔	✔	✔
26	✔	✔✔	✔	✔✔	✔
27	✔	✔✔	✔	✔✔	
28	✔	✔	✔	✔✔	
29	✔	✔✔	✔	✔	
30		✔		✔	✔✔
31	✔	✔✔	✔✔	✔	✔
32		✔✔	✔✔		
33	✔✔	✔✔	✔		

Now we have a defense-in-depth approach to protect our network. NIST has provided us with a framework we can use as a guideline for security throughout the entire system life cycle. Next we need to determine what type of operating system platform to use for our major applications. Well, there are many choices. Should we go with a Windows system? The Microsoft (MS) platforms have great GUI interfaces and numerous applications, but patch after patch needs to be applied to keep attackers from exploiting vulnerabilities that are discovered each week.

Well, we could go with freeware such as Linux. Linux has great security features and seems to require less patching than Microsoft products. Linux also seem to be less vulnerable to viruses. But on the down side Linux requires very experienced system administrators to partition, configure and install the operating system. Security personnel and/or system administrators must be extremely familiar with shell commands, shell scripts, source code, daemons and file system structures to shut down all the unneeded services that are running when doing a fresh operating system install. This is all so confusing but luckily we have an agency to consult.

The National Security Agency (NSA) History & Authority:

President Harry S. Truman established the National Security Agency (NSA) in 1952 and the NSA is separately organized agency within the Department of Defense (DOD). NSA plans, coordinates, directs and performs foreign signals intelligence and information security. NSA is a high-technology organization, working on the "cutting edge" of communications and data processing. The expertise and knowledge it develops provide the US government with systems that deny foreign powers knowledge of its capabilities and intentions.

> The [NSA] information systems security mission provides leadership, products, and services to protect classified and unclassified national security systems against exploitation through interception, unauthorized access, or related technical threats. Under a Presidential directive in 1984 the NSA was assigned responsibility for computer security and with an operations security-training mission in a 1988 Presidential directive.

The National Security Agency has recently declassified and released "how to" documentation on securing several information systems. The System and Network Attack Center (SNAC), a division of the NSA, is responsible for providing this extensive research and documentation. Among the documentation are numerous Windows 2000 security recommendation guides and guides to the secure configuration of IP routers. Documentation on securing the Linux open source operating system is also provided.

The documentation on the Windows 2000 operating system is extensive and is too numerous to try to discuss individually in any depth. Most Window 2K guides are in Adobe Acrobat and cover such topics as network architecture, securing group policy, securing active directory, securing domain name servers, securing the encrypting file system, configuration and administration of the ISA server, securing certificate services, PKI in Outlook 2000, IIS 5.0,

Kerberos settings, and Windows 2K router configuration. The URL is provided below:

http://nsa1.www.conxion.com/win2k/index.html

As most of us know, routers are the traffic cops of computer networks. Routers direct and control data flowing across networks and the Internet. Network administrators and security officers work in conjunction to secure network perimeters. They use routers to control network access, ward-off attacks, and restrict access to other subnets. Network administrators are concerned with managing connections within their network. Network administrators are also concerned with connections between their network and other networks. When it comes to routers, security officers are concerned more with defending the perimeters of the network from intruders and restricting access to unauthorized individuals. The security officer works in conjunction with the network administrator so the configuration of the routers, firewalls and intrusion detection devices work in harmony. The routers and firewalls are the proverbial beefeaters of the entire network.

NSA has also declassified and released SNAC research on IP router configuration, with an emphasis on Cisco routers. This guide gathered questions from IT professionals concerning routers, used the questions as a resource and addressed them in the "Router Security Configuration Guide". SNAC suggests that you always keep an offline copy of the router configuration file. If a suspected network intrusion occurs you can compare the offline configuration file with the online version to detect any changes or discrepancies. Access filter lists should be implemented and only permit protocols and services that the users truly need. Always use the "law of least privileges" when installing routers and firewalls. Always turn off router services that are not needed. Unusual or unwanted traffic to the router should be logged and monitored to detect patterns of possible attacks. The SNAC document is packed full security tips and practices. The URL is listed below:

http://nsa1.www.conxion.com/cisco/index.html

NSA has also undertaken the task of securing the open source operating system Linux. The Linux system is a variation of the UNIX system that can be run on a home computer or used in a multi-faceted environment.

http://www.nsa.gov/selinux/index.html

National Information Assurance Partnership (NIAP):

The National Information Assurance Partnership (NIAP) is collaboration between the National Institute of Standards and Technology and the National Security Agency. NIAP is tasked with meeting the needs of both the information technology.

> The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP helps both NIST and NSA in fulfilling their respective responsibilities under the Computer Security Act of 1987. The

partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure.

The NIAP website has numerous product reviews and assessments. Products listed by company and country make it easy for the system administrator and security offier to select the proper products for their network

CONCLUSION:

The United States Federal government has enacted laws, delegated authority, and placed responsibility in its agencies to provide guidelines for securing information systems. Under the Department of Commerce, the National Institute of Standards and Technology (NIST) develops national standards for information technology and serves as the guiding light to Federal agencies. NIST takes Congressional legislation regarding information systems and creates benchmarks / guidelines for governmental and non-governmental agencies to follow. NIST continues to provide products, standards, measurements and information system security guidelines for government and non-government agencies.

BIBLIOGRAPHY

Systems Administration and Network Security (SANS).
URL: http://www.incidents.org/isw/iswp.php#background (16 August 2001)

Host, Robert. "New Information Security Requirements for Federal Agencies". 5 February 2001. URL: http://www.sans.org/infosecFAQ/policy/fed.htm (25 July 2001).

Gebler, Dan. "U.S. Government Computers Widely Hacked in 2000". NewsFactor Network. 6 April 2001. URL: http://www.newsfactor.com/perl/story/8758.html

Office of Management and Budget. "Security of Federal Automated Information Resources." Appendix III, OMB Circular No. A-130, Transmittal IV. 28 November 2000.
URL: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html (20 March 2001)

National Institute of Standards and Technology (NIST). "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)" Special Publication 800-27. June 2001 URL: http://csrc.nist.gov/publications/nistpubs/ (25 July 2001).

National Institute of Standards and Technology (NIST). "Information Technology Bulletin" June 2001.
URL: http://www.itl.nist.gov/lab/bulletns/bltnjun01.pdf

Bush, George. "Presidential Memo on the 100th Birthday of NIST"
http://www.nist.gov/public_affairs/presidential_message.htm

National Security Agency (NSA).
URL: http://nsa1.www.conxion.com/win2k/index.html (25 July 2001).

URL: http://nsa1.www.conxion.com/cisco/index.html (16 August 2001).

URL: http://www.nsa.gov/selinux/index.html

National Information Assurance Partnership (NIAP)
URL: http://niap.nist.gov/cc-scheme/ValidatedProducts.htm

106th United States Congress. "FY 2001 Defense Authorization Act (P.L. 106-398)". 30 Oct. 2000 http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=publ398.106&directory=/disk3/wais/data/106_cong_public_laws (16 August 2001)