GIAC
CERTIFICATIONS

# 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 permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

# The Changing Face of Federal Information Technology Security:
## *Driving Legislation Behind IT Security in the Public Sector*

The mission of any enterprise network security organization is to protect the confidentiality, integrity, and availability of information residing on, or processed by, the organizations automated information systems (AIS). An agency's AIS can include any or all of the following: mainframe, midrange and microcomputer systems, personal computer workstations, laptops, local and wide area networks (intranets), and the Internet.

The nation's economy has grown increasingly dependent upon information technology (IT) networks and systems. As these systems are extremely vulnerable to malicious attacks and/or disruptions, the Government has initiated an aggressive and exhaustive campaign to repair federal systems and work hand-in-hand with private industry in an effort to secure the nation's critical information systems. Potential threats to our critical information systems are more significant than initially perceived. And as the dependency on AIS increases, so does the presence of our adversaries, as well as their ability to disrupt our networks and systems.

In such an ever changing technological environment, it is imperative that both the government and industry not only increase the level of security for the nation's current IT systems and networks, but also ensure that such security measures are incorporated into "next generation" networks and systems. Top priority must be given to the securing of our nation's critical infrastructure if we are to continue to prosper in the future.

To be a successful IT security professional in the public sector requires understanding the basic legislation and policies that form the security programs that protect Federal systems. This paper provides a summary of the key laws and guidelines that have been issued by the Federal government for the protection of the public infrastructure. This list is in no way comprehensive, but includes the fundamental legislation and the recently updated guidelines.

**Background:**

Data, and information, security encompasses three fundamental areas:

- Confidentiality – protecting sensitive data from unauthorized disclosure
- Integrity – ensuring data remains accurate throughout its life cycle
- Availability – ensuring data be ready for use by end users when needed

Data is secured because it is potentially valuable or potentially dangerous. The use of intranet or internet communications by an agency poses significant risks to data. Data confidentiality is threatened in two ways. First, since internet communications use common carrier telecommunications lines, it becomes possible for "outside" users to become a part of the network. This is generally called "hacking" and hacking is the source of many evils. The second threat relates to data while in transit, which is out of the control of the agency. This poses a significant risk of compromise.

The national posture on the vision of security was heightened by the Critical Infrastructure Protection Presidential Decision Directive 63, which was issued May 22, 1998. The directive called for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the country. Such infrastructures include telecommunications,



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

banking and finance, energy, transportation, and essential government services. This directive required federal government action, including risk assessment and planning to reduce exposures.

**The Legislation:**

Congress has been busy since the issuance of PDD 63, drafting and issuing legislation to strengthen the Government's posture on IT security, as well as fortifying its ties to private industry. The General Services Administration (GSA) has been directed to provide updates on IT legislation under consideration by Congress. What follows is a brief list of the major legislation affecting IT security and highlight of their requirements.

**OMB Circular A-130**

The directive that establishes policy for the management of Federal information resources is the Office of Management and Budget's Circular A-130. In particular, Appendix III, Security of Federal Automated Information Resources. Circular A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

A-130 establishes many basic considerations and assumptions, including:

- Government information is a valuable national resources;
- The free flow of information between the government and the public is essential to a democratic society;
- The management of Federal information resources should protect the public's right of access to government information;
- The individual's right to privacy must be protected;
- The Federal Government must cooperate with state and local governments in the management of information resources; and
- Users of Federal information resources must have skills, knowledge, and training to manage information resources.

OMB recently issued "Transmittal 4", a revision to A-130, Management of Federal Information Resources, to incorporate provisions of OMB A-11 and Clinger-Cohen Act, which is also known as the Information Technology Management Reform Act of 1996. The transmittal modifies the areas of information systems and information technology management so that they more closely follow the Clinger-Cohen Act. The modified areas involve:

1. resource planning to support the strategic missions;
2. implementing a capital plan that links to the budget; and



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. restructuring/rethinking how an agency does their work before investing in information systems.

Agencies must ensure that security is incorporated into their systems and that it is included in the budgets for information systems. Security controls must be consistent with the agency's enterprise architecture, and incorporate security plans that comply with federal standards.

The agency's Chief Information Officer (CIO) is responsible for advising the agency head on all information resource activities, such as development and system implementation. The CIO will also be responsible for monitoring and ensuring that a capital planning process is in place for all information resources.

In addition, agencies must provide a way for information to be disseminated to the public. Agencies should create a handbook that describes in one place the various ways by which a person can access public information from the agency as well as the type of information that is available. It should inform the public that information can be obtained electronically, through publications or through FOIA requests.

Transmittal 4 also requires that when selecting new products to enhance current systems or replace existing ones, they will need to be thoroughly researched and tested to ensure that they are compatible with existing systems or software which are already in use. In addition, security must be included at the start of a system's software development life cycle process. Finally, agencies must ensure that systems have security plans which are in accordance with Appendix III of A-130 and NIST guidelines (see below).

**Government Paperwork Elimination Act (GPEA) (October 1998)**

The Government Paperwork Elimination Act (GPEA) requires Federal agencies to allow individuals or entities that deal with the agencies the option to submit information and to maintain records electronically, when feasible. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives. This capability should be in place at each agency by October 21, 2003.

The GPEA requires the Director of the Office of Management and Budget:

- To provide direction and oversee the acquisition and use of information technology as a substitute for paper and for the use and acceptance of electronic signatures
- To develop procedures for the use and acceptance of electronic signatures by executive agencies
- To ensure that, within five years, executive agencies provide for the option of electronic maintenance, submission, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures, when practicable.
- To develop procedures to permit private employers to store and file electronically with executive agencies forms containing information pertaining to employees



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- In cooperation with the National Telecommunications and Information Administration, to conduct and report the Congress on an ongoing study of the use of electronic signatures on paperwork reduction and electronic commerce, individual privacy, and the security and authenticity of transactions.

Federal agencies should develop and implement plans, supported by an assessment, on the practicality of the use of electronic records. Each agency was to develop a plan by October 2000 that provides for continued implementation by the end of Fiscal Year 2003, of optional electronic transaction of information in substitute for paper.

**NIST Special Publication 800-25: Federal Agency User of Public Key Technology for Digital Signatures and Authentication (October 2000)**

As set forth by the GPEA, Federal agencies are encouraged to use public key technology. NIST 800-25 was developed by the Federal Public Key Infrastructure (PKI) Steering Committee to give guidance and to assist Federal agencies that are considering the use of public key technology for digital signatures or authentication over open networks such as the Internet.

Parties should have the assurance that their electronic communication is protected and cannot be altered once it has occurred. Also, that their identities are established separately, as to display where data has been created and where it is going, and that they cannot be impersonated. PKI technology enables software programs to guarantee such protection.

To help the public become comfortable with PKI technology, agencies would be wise to implement a public information plan, detailing the strengths of PKI technology, such as its time savings, cost savings, enhanced services and improved quality of data; costs in implementing the technology; and discuss any risks involved with its use and ways to minimize said risks. Agencies must decide if the risks are proportionate with their obligations to the public and the law. Possible risks are: fraud, service failure and liability. Agencies must consider this simple premise: how does the level of risk introduced by the PKI technology compare to the level of risk already in place, without said technology. With all the possible benefits that can be realized with PKI technology, the risks may be far outweighed by the advantages created.

**Government Information Security Reform Act (October 2000)**

One of the most important acts to come out last year was the Government Information Security Reform Act (GISRA). The purposes for the issuance of the GISRA include providing a comprehensive framework for establishing and ensuring effective controls over Federal IT resources, ensuring interoperability between Federal systems is achieved in the most cost-effective manner, providing for the development and maintenance of controls required to protect Federal information systems, and providing a mechanism for improved oversight of Federal agency information security programs.

GISRA establishes authorities and responsibilities for Federal agencies, and directs the heads of agencies to:

- identify, use, and share best practices;
- develop an agency-wide information security plan;



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- incorporate information security principles and practices throughout the life cycles of the agency's information systems; and
- ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems.

The Act reinforces the requirements for each agency to develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by the agency. In addition, agencies must ensure that their information security plan is practiced throughout the life cycle of each system. One of the major changes that the GISRA makes to the existing legislation is the addition of authentication and non-repudiation to the requirement of ensuring the integrity, confidentiality, and availability of information and information systems supporting agency operations and assets. Authentication and non-repudiation introduce the requirement for encryption and/or digital signatures into the security process.

Each year each agency is now required to perform an independent evaluation of the information security program and practices of that agency. The evaluation must test the effectiveness of information security control techniques for the agency's information systems and an assessment of the compliance with Federal legislation and related information security policies, procedures, standards, and guidelines.

**FIPS Publication 140-2**

As a result of the GISRA's requirements of authentication and non-repudiation, Federal Information Processing Standard Publication 140-2 was released as a standard to be used by Federal agencies when cryptographic-based security systems are to be used to protect sensitive or valuable data. The standard presented for cryptographic modules, which are defined as a set of hardware, software and firmware, or a combination thereof that implements cryptographic logic or processes, describes four increasing, qualitative levels of security. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover the areas of design and implementation. The security level of the module is to be tied to the security requirements of the application and the environment.

Security Level 1 provides the lowest level of security, and specifies basic security requirements for a cryptographic module. Level 2 builds on Level 1 by adding the requirement for tamper-evident coatings or seals, or for pick-resistant locks – physical security for Level 1. This level requires role-based authentication. Security Level 3 attempts to prevent the intruder from gaining access to critical security parameters held within the cryptographic module by requiring identity-based authentication, which is stronger than the role-based authentication of Level 2. Security Level 4 provides the highest level of security, where physical security provides an envelope of protection around the cryptographic module to detect a penetration.

The publication provides for testing against the stated security requirements at each level of security, and describes the interfaces for data input and output. It describes acceptable authentication mechanisms, such as biometrics, passwords, PINs, cryptographic keys, and



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

tokens, and requires the documentation to provide descriptions of the chosen authentication mechanisms at each level of security.

**Conclusion**

The selection of IT security legislation above represents just the tip of an iceberg that is constantly under change. New legislation is issued almost weekly by Congress, as are guidelines by other Federal agencies. There are many other ancillary laws, guidelines, and publications that direct the protection of the Federal information security infrastructure. These include:

- FIPS PUB 46-3, Data Encryption Standard (DES), issued 25 October 1999
- M-01-05 (Memorandum for Heads of Executive Departments and Agencies), Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, issued 20 December 2000
- M-01-08 (Memorandum for Heads of Executive Departments and Agencies), Guidance on Implementing the Government Information Security Reform Act, issued 16 January 2001
- Records Management Guidance for Agencies Implementing Electronic Signature Technologies, issued 18 October 2000

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



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Bibliography/References**

100th Congress of the United States (Sponsor, Rep. Glickman). "Computer Security Act of 1987." Public Law 100-235, H.R.145. 8 January 1988. URL: http://thomas.loc.gov/bss/d100/d100laws.html (20 March 2001)

104th Congress of the United States (Sponsor, Sen. Thurmond). "Information Technology Management Reform Act of 1996." Public Law 104-106, s.1124. 10 February 1996. URL: http://thomas.loc.gov/bss/d104/d104laws.html (21 March 2001)

Federal Information Processing Standard Publication (FIPS PUB) 140-2. "Security Requirements for Cryptographic Modules." November 1999. URL: http://csrc.nist.gov/publications/fips/dfips10-2.doc (28 March 2001)

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)

106th Congress of the United States (Sponsor, Rep. Jim Gibbons). "Government Information Security Reform Act." Public Law 106-298, Subtitle G. 30 October 2000. URL: http://thomas.loc.gov/bss/d106/d106laws.html (20 March 2001)

National Institute of Standards and Technology. "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication." NIST Special Publication 800-25. October 2000. URL: http://ois.nist.gov/pub/nistpubs/nistpubs.html (24 March 2001)

104th Congress of the United States of America. "Information Technology Management Reform Act (Clinger/Cohen Act)." s.1124. 3 January 1996. URL: http://www.ed.gov/offices/OCIO/legislation/clinger_cohen.html (28 March 2001)

National Institute of Standards and Technology. "Guide for Developing Security Plans for Information Technology Systems." NIST Special Publication 800-18. December 1998. URL: http://ois.nist.gov/pub/nistpubs/nistpubs.html (24 March 2001)

105th Congress of the United States of America. "Government Paperwork Elimination Act." Public Law 105-277. 23 October 1998. URL: http://www.ed.gov/docs/gpealaw.htm (25 March 2001)

"Records Management Guidance for Agencies Implementing Electronic Signature Technologies." 18 October 2000. URL: http://www.nara.gov/records/policy/gpea.html (22 March 2001)

"Federal Privacy Legislation Table." 29 March 2001. URL: http://www.privacyheadquarters.com/legwatch/fedchart.html (1 April 2001)

"Sen. Wyden Predicts Congress Will Pass a Privacy Bill This Year." 22 January 2001. URL: http://www.techlawjournal.com/privacy/20010122.asp (1 April 2001)



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |