# Global Information Assurance Certification Paper

**Name: Thanh Viet Do**

**Certification: GIAC Security Leadership Certificate (GSLC)**
**Practical Assignment Version: 1.0 (April 8, 2002)**
**Practical Assignment: Management Topics in Information Security**
**Practical Assignment Option: A**
**Submission Date: July 16, 2003**



**Title: Federal IT Security Training Requirements**

**Abstract:** Security awareness, training, and education are keys to establishing and maintaining a culture sensitive to IT security. Federal laws and regulations require agencies to implement an IT security training program with provisions for initial training, periodic refresher training, application specific training, and role-based training. Unfortunately many federal employees and contractors still receive minimal or no formal training. They must be appropriately trained to understand computer security and their responsibilities. Employee and contractor security awareness, training, and education is perhaps the most basic and certainly one of the most critical elements of any IT security program. Previously neglected and often overshadowed by operational demands, IT security awareness, training, and education program needs to be the cornerstone of IT security program. This paper will describe the federal requirements for an IT security training program.

**Federal IT Security Training Requirements**

*Introduction*

In order to protect the confidentiality, integrity, and availability of information in a tightly integrated network environment, federal agencies are mandated to ensure that all individuals involved in the use, support, and management of systems are appropriately trained to perform their functions. Because people are usually the weakest link in the information technology (IT) security chain, having an ongoing IT security training program in place can greatly reduce many risks which cannot be mitigated through technological or other automated methods.

*Federal Requirements for IT Security Training*

Federal laws and regulations mandate each agency to create a comprehensive IT security training program.

The Computer Security Act of 1987 was passed to force agencies "to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes." It was the first law that required agencies to provide training to all personnel.

In January 1992, the Office of Personnel Management (OPM) issued a revision to the federal personnel regulations that made the previously voluntary National Institute of Science and Technology (NIST) Special Publication (SP) 500-172 "*Computer Security Training Guidelines*" mandatory. This regulation, 5 CFR Part 930, "*Employees Responsible for the Management or Use of Federal Computer Systems*", subpart C "Training Requirement" mandates federal agencies to provide training as set forth in NIST guidelines. The OPM regulation requires:

- Initial training be provided to all new employees within 60 days of employment.
- Continuing training be provided whenever there is a significant change in the agency's IT security environment or procedures, or when an employee enters a new position which deals with sensitive information.
- Refresher training be provided to all employees periodically, based on the sensitivity of the information the employee handles.

The Office of Management and Budget (OMB) Circular A-130, "*Management of Federal Information Resources,*" Appendix III, "*Security of Federal Automated Information Resources,*" re-emphasizes these mandatory training requirements. The circular further requires that prior to granting access to IT applications and systems, all individuals must receive specialized training focusing on their IT security responsibilities and the established application or system rules.

The Government Information Security Reform Act (GISRA), which consolidated many federal security policies into a single law, mandated that federal agencies develop a comprehensive IT security training program. It assigns the agency Chief Information Officer (CIO) the responsibility of "[ensuring] that the agency has trained personnel sufficient to assist the agency in complying with the requirements." GISRA requires agencies to provide specialized training to personnel with significant responsibilities in information security, and security awareness training to all personnel, including contractors.

The Federal Information Security Management Act (FISMA) of 2002 updated and extended GISRA. Like GISRA, it requires agencies to provide training to personnel with significant responsibilities in information security, and security awareness training to all personnel, including contractors. It furthers mandates agencies to follow the security standards developed by NIST and to make use of NIST security tools, such as NIST SP 800-16.

*Three Levels of IT Security Training*

The OMB Circular A-130, as revised in 1996, also requires NIST to update SP 800-172. In April 1998, NIST updated its guidance for IT security training via SP 800-16 "Information Technology Security Training Requirements." SP 800-16 presents a conceptual framework for providing IT security training. It provides guidance for developing and strengthening an IT security training program that is "comprehensive, measurable and cost-effective".

According to NIST, learning is a continuum from awareness through training to education. Learning starts with awareness, then builds to training, and eventually evolves into education. NIST differentiates awareness, training, and education.

The goal of **awareness** is to bring attention to security issues. Through awareness, everyone should be able to recognize security concerns and respond appropriately. As such, awareness is required for everyone who is involved in the use, support, and management of the IT systems. The training is to make sure the users are aware of the system or application rules, their responsibilities, and their expected behavior.

The goal of **training** is to provide job-specific skills to deal with security issues. Everyone, except for the end-user, who is directly involved in the IT systems lifecycle should be provided specialized training. This group includes, but is not limited to, those who develop, design, manage, purchase, and audit IT systems. Training must focus on job functions, roles and responsibilities specific to individuals, and not on job titles. It also must recognize that individuals have unique backgrounds, and different levels of understanding, therefore, require customized training.

The goal of **education** is to develop the "ability and vision to perform complex and multi-disciplinary activities and the skills need to further the IT security profession and to keep pace with threat and technology changes" (NIST SP 800-16, p. 14). The aim is to create IT security professionals who can integrate all security skills of various functional areas. Because IT security is multidisciplinary in nature, requiring a wide spectrum of knowledge such as computer security, operations security, telecommunication security, physical security, personnel security and related security areas, education is intended for IT security professionals only.

*Implementing an IT Security Training Program*

Awareness, training, and education are three distinct components of an IT security training program. In order to implement a comprehensive training program, each of the three components must be addressed separately.

According to NIST, the goal of IT security awareness can easily be accomplished via poster, video, or newsletter. Unfortunately, FISMA also requires agencies to report statistics of how this requirement is accomplished. Therefore, agencies are required to track and ensure all end-users have the basic IT security awareness. Many agencies accomplish this reporting requirement by providing a web-based IT security awareness module, where the tracking capability can be implemented.

The goal of IT security training is to provide the skills necessary to those who are directly involved in the lifecycle of the systems. This can be accomplished through formal or on-the-job training. Again, because of reporting requirements, agencies are required to track and ensure all IT professionals complete the necessary training. It can be a daunting task trying to tailor each individual's needs to the individual requirement. Karta Technologies is one of the vendors that have a series of web-based IT security training courses to help many agencies meet the specialized IT security training needs. The catalog includes training plans for many IT roles. Karta Technologies offers courses with different levels of difficulty so IT professionals can complete those at their level of expertise. Most importantly, all the courses map back to the NIST SP 800-16 requirements for the different IT roles.

The goal of IT security education is provide a wide spectrum of knowledge in IT, including knowledge of security control concepts, computer hardware, software, telecommunications concepts, physical and logical security, data architecture, database management and data access methods, pertinent legislation, and administration and organizational issues. NIST SP 800-16 does not provide any criteria for IT security professionals. However NIST states, "To reach the advanced level of IT security professionalization, completion of formal education in the field is required." In other words, the IT security professionals should at

least have a bachelor's degree in the IT security field and/or a security certification (such as CISSP and GSEC) that covers a wide range of IT domains. They need to keep up to date with technologies, at least theoretically. This can be accomplished via studying, researching, or attending seminars.

*Conclusion*

A well designed IT security training program can help an agency reduces its risks. When implemented correctly, it becomes very effective security controls against the human risk factor.

## References


1. Computer Security Act of 1987, Public Law 100-235. http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf.
2. Federal Information Security Management Act (FISMA) of 2002, HR 2458. http://csrc.nist.gov/policies/FISMA-final.pdf.
3. Government Information Security Reform Act (GISRA), Public Law 106-398. http://thomas.loc.gov/cgi-bin/query/F?c106:1:./temp/~c1060aKcup:e869098.
4. Karta Technologies. http://itsl.ts.karta.com.
5. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16 "Information Technology Security Training Requirements: A Role- and Performance-Based Model", April 1998. http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf.
6. Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources." http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.
7. Office of Personnel Management 5 CFR Part 930, subpart C, "Training Requirement", January 3, 1992. http://csrc.nist.gov/secplcy/opm_plcy.txt.