CHAPTER 9, PART 1
COMPUTER SECURITY TRAINING AND AWARENESS

1 BACKGROUND

The Computer Security Act of 1987 defines users of IT systems and establishes minimum acceptable security practices for Federal computer systems: “Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practices of all persons who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.”

Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," establishes a minimum set of controls to be included in Federal IT security programs and assigns Federal agencies responsibility for security of automated information.

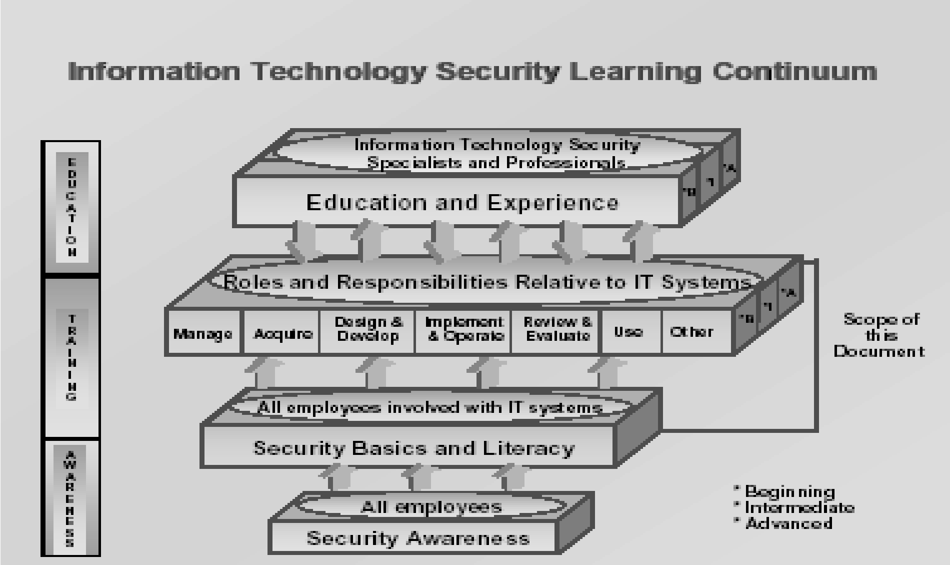
Hspd-7 provides key Federal policy elements on critical infrastructure protection. This directive specifies “there shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.”

The Federal Information Security Management Act (FISMA) mandates: general training of employees to ensure that they are aware of their security responsibilities; specialized training of agency employees with significant security responsibilities and reporting of agency statistics on security awareness and training efforts.

Security training and awareness requirements are described in 5 CFR 930, “Employees Responsible for the Management of Use of Federal Computer Systems,” and the National Institute of Standards and Technology (NIST) special Publication 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model,” dated April 1998. Executive

Order 13103, “Computer Software Piracy,” dated September 30, 1998, requires training on the prevention of software piracy; NIST Special Publication 800-18, “Guide for Developing Security Plans for Information Technology Systems,” December 1998, reiterates the requirement “to provide mandatory periodic training.”

Exhibit 2-1
IT Security Learning Continuum


Information Technology Security Learning Continuum
EDUCATION
TRAINING
AWARENESS
Information Technology Security Specialists and Professionals
Education and Experience
*B
*I
*A
Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design & Develop
Implement & Operate
Review & Evaluate
Use
Other
*B
*I
*A
Scope of this Document
All employees involved with IT systems
Security Basics and Literacy
All employees
Security Awareness
* Beginning
* Intermediate
* Advanced

The model presented as Exhibit 2-1 is based on the premise that learning is a continuum. Specifically, learning in this context starts with awareness, builds to training, and evolves into education. This model provides the context for understanding and using this document.

The model is role-based. It defines the IT security learning needed as a person assumes different roles within an organization and different responsibilities in relation to IT systems. This document uses the model to identify the knowledge, skills, and abilities an individual needs to perform the IT security responsibilities specific to each of his or her roles in the organization.

The type of learning that individuals need becomes more comprehensive and detailed at the top of the continuum. Thus, beginning at the bottom, all employees need awareness. The purpose of awareness presentations is to focus attention on security. Awareness relies on using attractive packaging techniques to reach broad audiences. Although more informal in nature, it is important to set the stage for security training in both the individual and organizational culture. The goal of awareness presentations is to mention security requirements, the problems they were designed to remedy and the desired response by the audience.

Training (represented by the two bracketed layers "Security Basics and Literacy" and "Roles and Responsibilities Relative to IT Systems" in Exhibit 2.1) is required for individuals whose role in the organization indicates a need for special knowledge of IT security threats, vulnerabilities, and safeguards. Training is more formal, having a goal of building knowledge and skills to facilitate job performance. IT Security Basics and Literacy is the transitional activity between Awareness and Training. It consists of relatively generic concepts, terms and associated learning models. End-user Security Training administered annually or for new hires is an example of this type of transitional activity. This training represents a baseline of IT security knowledge across government that all employees can reasonably be expected to have. Roles and Responsibilities training is directed toward courses that contain much of the same material found in a college or university course but are focused on the job responsibilities of IT professionals and those skills needed to execute them successfully. These courses are provided to individuals that are responsible for ensuring the security of all USDA IT systems.

The "Education and Experience" layer applies primarily to individuals who have made IT security their profession. Providing formal education to this group and on-the-job experience is desirable for IT Security Specialists to fulfill their roles in an effective manner. Education should be provided to other agency employees based on their security roles and responsibilities in the organization.

2 POLICY

This policy addresses only the awareness and training components of the IT Security Learning Continuum. All USDA agencies and staff offices will develop, organize, implement, and maintain an IT systems security awareness and training program to ensure the security of USDA information and IT resources and to establish requirements for security awareness and training to be conducted for all employees at least annually. The Department will establish a generic computer security awareness and training program for eventual use throughout USDA. This program will define the policy, strategy and sources for awareness and training within the department. However, each agency and staff office still has the responsibility for developing, conducting and implementing computer security awareness and training, even in the absence of a Departmental program.

NIST Special Publications 800-16 and 800-50 shall be the recommended sources for guidance and direction in the design of the computer security awareness and training program in each USDA agency and staff office. OPM Regulation Title 5, Volume 2, Parts 930.301-305 provides specific legal requirements to provide training. Each agency and staff office will also develop a Computer Security Awareness and Training Plan to serve as a working tool in the implementation of its internal program. NIST 800-50, Appendix B, has a sample plan that can serve as a model for development of an agency plan. The agency or staff office will send an electronic copy of its Security Awareness and Training Plan to CS for review and comment annually .

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. CS will monitor all approved exceptions.

3 PROCEDURES

All USDA personnel involved in the management, use, design, development, maintenance or operation of an application or automated information system shall be made aware of their security responsibilities based on their level of access to systems and data (need-to-know) and trained to fulfill them. Training content shall assure that all groups specified above are versed in the rules and requirements pertaining to security of the respective Federal IT systems, which they access, operate, or manage.

Training shall be consistent with guidance issued by the OMB and NIST Special Publication 800-16. New employees shall be trained within 60 days of hire. Computer security refresher training is required at least annually or whenever there is a significant change in IT direction, major system modifications, changes/upgrades in software utilized, or change of duties for continued access to USDA IT systems. All agency employees will sign a Computer User Security Agreement. These agreements will list key computer security policies/objectives and legal references. All agencies/staff offices will retain copies of a signed Computer User Security Agreement from employees receiving initial or annual computer security awareness and training. The immediate supervisor will retain the original agreement; a copy will be given to the employee and electronic training notification will be given to the agency ISSPM by the immediate supervisor. This notification will include the employee name, course title and date trained. Agency internal awareness and training programs will be subject to oversight reviews by Cyber Security (CS) and the training statistics will be reported in the annual Agency Overall Security Plan and Government Information Security Reform Act (GISRA) documents by each agency and staff office.

Training must include software piracy prevention and appropriate software use training in compliance with Executive Order 13103, "Computer Software Piracy." USDA agencies and staff offices will distribute security alerts and advisories from reliable sources, as needed and through appropriate media, to remind all groups of security practices or to inform them of new security issues. Training shall be conducted during new employee orientation or as soon as possible after beginning of employment. Security awareness and training will be conducted for contractors, subcontractors, grantees, and co-operators as soon as possible after the contract or agreement is effective. Signed original Computer User Security Agreements will be maintained by the agency ISSPM for these groups; a copy will be provided to the group member trained. The agency ISSPM will prepare electronic summary statistics for GISRA reporting. Security awareness and training should be made part of regularly scheduled IT training classes. USDA agencies and staff offices are encouraged to collaborate and work together to share training resources, reduce costs, share information, and accelerate delivery of training.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Provide guidance and strategies to assist USDA agencies in complying with Public Laws and Federal regulations, and department guidelines relating to Computer Security Awareness and training and overlapping issues, such as ethics, privacy and communications. This guidance will delineate the differences between awareness and training;

(2) Work with agencies and staff offices to ensure compliance with Federal laws and regulations related to information security training and awareness;

(3) Develop a Department-wide Computer Security Awareness and Training Program for use by agencies/staff offices; and

(4) Perform oversight reviews of agencies/staff offices internal training plans to ensure compliance with this policy.

b <u>Agency Management and Information Technology Officials or Chief Information Officer will:</u>

(1) Establish a formal computer awareness and training program consistent with guidance issued by NIST and OMB using an agency or department sponsored contractual agreement or in-house developed program;

(2) Conduct computer security awareness and training sessions in the form of seminars, interactive electronic-based training, demonstrations, or hands-on training; prepare a formal agency Computer Security Awareness and Training Plan for the overall organization and reference in overall agency security plan;

(3) Additional informal awareness presentations will be conducted on a frequent basis in addition to formal training in the form of additional electronic media, video presentations, hard copy reading materials, and posters;

(4) Periodic reviews of training material and methods will be conducted with training vendors to ensure that training is current and relevant;

(5) Maintain an overall electronic system for tracking statistical training performance measures required by FISMA and send annually to CS on or before July 31st;

(6) Ensure that all users are appropriately trained to fulfill security responsibilities based on their need-to-know, before allowing them access to any USDA information system; this training should include legal use of software, licensing agreements and restrictions of limited personal use of government IT assets;

(7) Ensure policies and procedures include the training of employees, contractors, subcontractors, grantees and co-operators in records management, protection of privacy, and other security safeguards;

(8) Implement compliance and evaluation processes as part of the organization's IT security awareness and training program;

(9) Each agency will also ensure that employees sign a written certification (Computer User Security Agreement) that they have been trained and made aware of the security rules and regulations after security training is administered; the employee's supervisor is to maintain the original copy of the certification and a copy of the certification will be provided to the employee;

(10) Ensure that electronic notification of this training (employee orientation, refresher, or specialized) is sent to the agency ISSPM. This notification will include name(s) of individual trained, date, and course title. The original copy of the certifications of other groups (contractors, subcontractors, co-operators, grantees) training is also to be maintained by the ISSPM;

(11) Ensure that all agency instructors have received and satisfactorily completed "Train the Trainer" or equivalent instruction;

(12) Encourage employees to request additional IT Security training based on their responsibilities and

plan for training through the Individual Development Plan (IDP) process;

(13) Include computer security training requirements in all new procurement requests, specifications, statements of work, grants and cooperative agreements to reflect the appropriate level of awareness and training based on job functions and access required; and

(14) Administer New Employee Orientation to include IT Computer Security training.

c <u>The Office of the Chief Financial Officer will:</u>

Issue guidance to ensure all new grants and cooperative agreements to reflect the requirements of this policy/procedures.

d <u>The agency Information Systems Security Program Managers will:</u>

(1) Work with the appropriate agency management officials to establish a program that provides computer security awareness and training to all users of USDA IT systems in accordance with NIST and OMB guidance;

(2) Ensure this program incorporates physical security practices contained in DM 3510-001, Chapter 2, Part 1, Security Standards for Information Technology (IT) Restricted Space to protect IT resources from damage, loss, and prevent unauthorized access to agency information resources;

(3) Identify, develop, and support methods for dissemination of computer security awareness and training; promote the ethical use of information resources within the agency;

(4) Participate in the annual review and redesign the security awareness program in cooperation with agency training vendors to assure that training is relevant and current; prepare the overall Agency Computer Security Awareness and Training Plan, as necessary;

(5) Coordinate with agency personnel generating procurement requests, grants and service agreements to ensure that these types of documents include security awareness and training requirements for contractors, subcontractors, grantees, and cooperators;

(6) Work with managers to ensure they understand the requirements in NIST Special Publications 800-16 and 800-50;

(7) Maintain electronic or hardcopy records of employees, contractors, subcontractors, grantees and co-operators trained; ensure training statistics are included in the annual GISRA report; and

(8) Conduct periodic agency security training compliance reviews to ensure records are accurate.

e <u>USDA Employees, Contractors, Subcontractors, Grantees and Cooperators will</u>:

(1) Attend agency-sponsored computer security awareness and training and refresher seminars mandated by law and identified by supervisors or agency project managers;

(2) Become familiar with the major implications of licensed software agreements;

(3) Recognize and report suspected security incidents to the agency ISSPM and the immediate supervisor/project manager in cases of suspected

abuse of USDA computer resources, understanding that all reports shall be kept confidential; and

(4) Be familiar and comply with the established USDA and Agency security policies and practices, and sign a written certification (user acknowledgement) that they have been trained and made aware of the security rules and regulations.

-END-