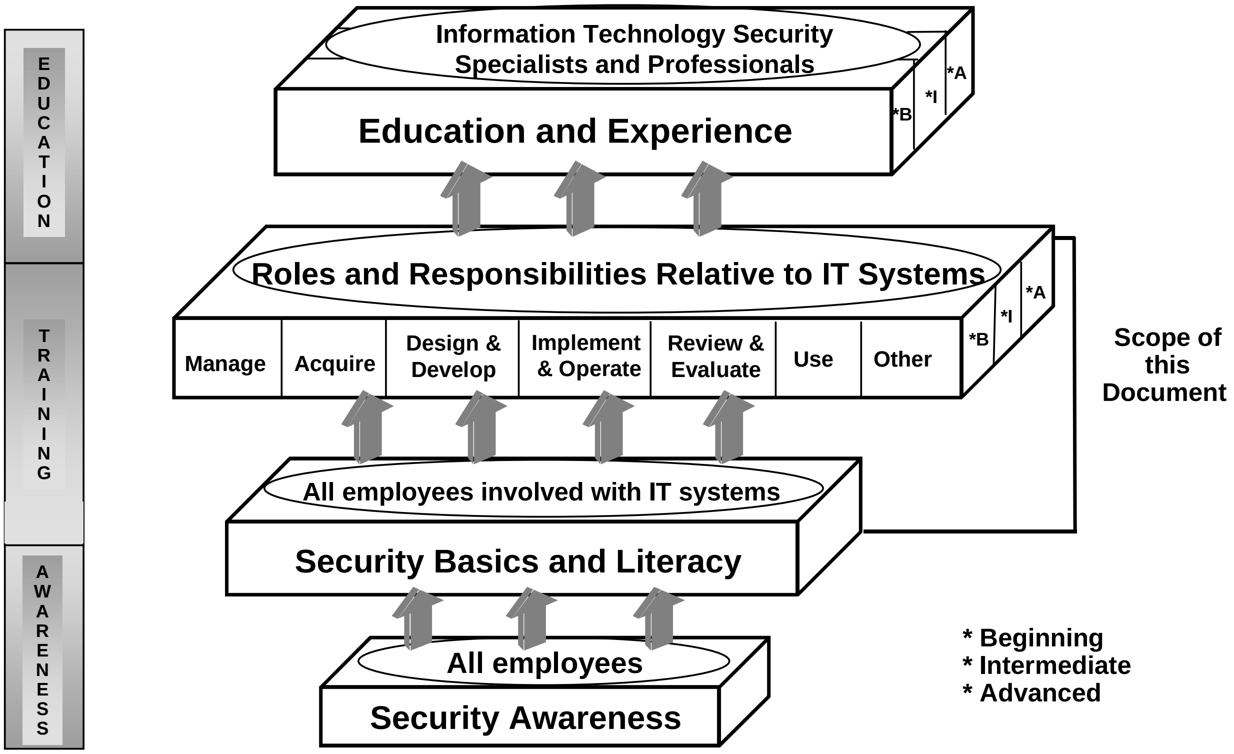
APPENDIX A

APPENDIX A — LEARNING CONTINUUM



APPENDIX
B

APPENDIX B — IT SECURITY TRAINING MATRIX

		FUNCTIONAL SPECIALTIES						
TRAINING AREAS		A MANAGE	B ACQUIRE	C DESIGN & DEVELOP	D IMPLEMENT & OPERATE	E REVIEW & EVALUATE	F USE	G OTHER
1	LAWS & REGULATIONS	1A	1B	1C	1D	1E	1F	▨
2	SECURITY PROGRAM							
2.1	PLANNING	2.1A	2.1B	2.1C	2.1D	2.1E	▨	▨
2.2	MANAGEMENT	2.2A	2.2B	2.2C	2.2D	2.2E	▨	▨
3	SYSTEM LIFE CYCLE SECURITY							
3.1	INITIATION	3.1A	3.1B	3.1C	▨	3.1E	3.1F	▨
3.2	DEVELOPMENT	3.2A	3.2B	3.2C	3.2D	3.2E	3.2F	▨
3.3	TEST & EVALUATION	▨	▨	3.3C	3.3D	3.3E	3.3F	▨
3.4	IMPLEMENTATION	3.4A	3.4B	3.4C	3.4D	3.4E	3.4F	▨
3.5	OPERATIONS	3.5A	3.5B	3.5C	3.5D	3.5E	3.5F	▨
3.6	TERMINATION	3.6A	▨	▨	3.6D	3.6E	▨	▨
4	OTHER	▨	▨	▨	▨	▨	▨	▨

The “bricked” cells are null sets at this time.

APPENDIX C

APPENDIX C — GLOSSARY

NOTE: The following terms are defined for use throughout this document.

Acceptable Risk — the level of *Residual Risk* that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. *(See Total Risk, Residual Risk, and Minimum Level of Protection.)*

Accreditation — also known as *authorize processing* (OMB Circular A-130, Appendix III), and *approval to operate*. Accreditation (or authorization to process information) is granted by a management official and provides an important quality control. By accrediting a system or application, a manager accepts the associated risk. Accreditation (authorization) must be based on a review of controls. *(See Certification.)*

Acquisition, Development, and Installation Controls — the process of assuring that adequate controls are considered, evaluated, selected, designed and built into the system during its early planning and development stages and that an on-going process is established to ensure continued operation at an acceptable level of risk during the installation, implementation and operation stages.

Adequate Security — security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, acquisition, development, installation, operational, and technical controls.

Application — the system, functional area, or problem to which information technology is applied. The application includes related manual procedures as well as automated procedures. Payroll, accounting, and management information systems are examples of applications.

Approval to Operate — see *Certification* and *Accreditation.*

Automated Information System Security — synonymous with *Information Technology Security.*

Automated Information System Security Program — synonymous with *IT Security Program.*

Availability — the timely, reliable access to data and information services for authorized users.

Awareness — a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

Awareness, Training, and Education Controls — include (1) awareness programs which set the stage for training by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure, (2) training which teaches people the skills that will enable them to perform their jobs more effectively, and (3) education which is targeted for IT security professionals and focuses on developing the ability and vision to perform complex, multi-disciplinary activities.

Baseline Security — the minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.

Behavioral Outcome — what an individual who has completed the specific training module is expected to be able to accomplish in terms of IT security-related job performance.

Certification — a formal process for testing components or systems against a specified set of security requirements. Certification is normally performed by an independent reviewer rather than one involved in building the system. Certification *can be* part of the *review of security controls* identified in OMB Circular A-130, Appendix III, which calls for security reviews to assure that management, operational, and technical controls are appropriate and functioning effectively. *(See Accreditation.)*

Computer Security — synonymous with *Information Technology Security.*

Computer Security Program — synonymous with *IT Security program.*

Confidentiality — the assurance that information is not disclosed to unauthorized individuals or processes.

Education — IT security education focuses on developing the ability and vision to perform complex, multi-disciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

FISSEA — the *Federal Information Systems Security Educator's Association*, an organization whose members come from federal agencies, industry, and academic institutions devoted to improving the IT security awareness and knowledge within the federal government and its related external workforce.

Information Sharing — the requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs.

Information Systems Security — synonymous with *IT Security*.

Information Systems Security Program — synonymous with *IT Security Program.*

Information Technology (IT) — computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit, or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software. See also *IT System* and *IT Security*.

Integrity — the quality of an IT system that reflects the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implements the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

IT Security — technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. Synonymous with *Automated Information System Security, Computer Security and Information Systems Security*.

IT Security Basics — a core set of generic IT security terms and concepts for all federal employees as a baseline for further, role-based learning.

IT Security Body of Knowledge Topics and Concepts — a set of 12 high-level topics and concepts intended to incorporate the overall body of knowledge required for training in IT security.

IT Security Literacy — the first solid step of the IT security training level where the knowledge obtained through training can be directly related to the individual’s role in his or her specific organization.

IT Security Program — a program established, implemented, and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its information technology systems. Synonymous with *Automated Information System Security Program, Computer Security Program, and Information Systems Security Program.*

IT System — a collection of computing and/or communications components and other resources that support one or more functional objectives of an organization. IT system resources include any IT component plus associated manual procedures and physical facilities that are used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating procedures. An IT system may consist of one or more computers and their related resources of any size. The resources that comprise a system do not have to be physically connected.

Job Function — the roles and responsibilities specific to an individual, not a job title.

Knowledge Levels — verbs that describe actions an individual should be capable of performing on the job after completion of the training associated with the cell. The verbs are identified for three training levels: Beginning, Intermediate, and Advanced.

Laws and Regulations — federal government-wide and organization-specific laws, regulations, policies, guidelines, standards, and procedures mandating requirements for the management and protection of information technology resources.

Learning — knowledge gained by study (in classes or through individual research and investigation).

Learning Continuum — a representation in which a the common characteristic of learning is presented as a series of variations from awareness through training to education.

Learning Objective — a link between the verbs from the "knowledge levels" section to the "Behavioral Outcomes" by providing examples of the activities an individual should be capable of doing after successful completion of training associated with the cell. Learning Objectives recognize that training must be provided at Beginning, Intermediate, and Advanced levels.

Likert Scale — an evaluation tool that is usually from one to five (one being very good; five being not good, or vice versa), designed to allow an evaluator to prioritize the results of the evaluation.

Management Controls — management controls are actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures, and rules of behavior, individual roles and responsibilities, individual accountability and personnel security decisions.

Minimum Level of Protection — the reduction in the *Total Risk* that results from the impact of in-place safeguards. *(See Total Risk, Acceptable Risk, and Residual Risk.)*

Operational Controls — the day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment.

Performance-Based — a method for designing learning objectives based on behavioral outcomes, rather than on content that provides benchmarks for evaluating learning effectiveness.

Residual Risk — the potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. *(See Total Risk, Acceptable Risk, and Minimum Level of Protection.)*

Risk — the probability that a particular security threat will exploit a system vulnerability.

Risk Management — the on-going process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Roles and Responsibilities — functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

Role-Based — mapped to job function, assumes that a person will take on different roles, over time, within an organization and different responsibilities in relation to IT systems.

Sensitivity — the degree to which an IT system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components.

System — see *IT System*.

System Environment — the unique technical and operating characteristics of an IT system and its associated environment, including the hardware, software, firmware, communications capability, organization, and physical location.

System Interconnection — the requirements for communication or interconnection by an IT system with one or more other IT systems or networks, to share processing capability or pass data and information in support of multi-organizational or public programs.

Technical Controls — hardware and software controls used to provide automated protection to the IT system or applications. Technical controls operate within the technical system and applications.

Threat — an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Total Risk — the potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). *(See Acceptable Risk, Residual Risk, and Minimum Level of Protection.)*

Training — teaching people the knowledge and skills that will enable them to perform their jobs more effectively.

Training Assessment — an evaluation of the training efforts.

Training Effectiveness — a measurement of what a given student has learned from a specific course or training event, i.e., learning effectiveness; a pattern of student outcomes following a specific course or training event; i.e., teaching effectiveness; and the value of the specific class or training event, compared to other options in the context of an agency's overall IT security training program; i.e., program effectiveness.

Training Effectiveness Evaluation — information collected to assist employees and their supervisors in assessing individual students' subsequent on-the-job performance, to provide trend data to assist trainers in improving both learning and teaching, and to be used in return-on-investment statistics to enable responsible officials to allocate limited resources in a thoughtful, strategic manner among the spectrum of IT security awareness, security literacy, training, and education options for optimal results among the workforce as a whole.

Training Matrix — a table that relates role categories relative to IT systems—Manage, Acquire, Design and Implement, Operate, Review and Evaluate, and Use (with a seventh category, "other" included to provide extensibility) with three training content categories—Laws and Regulations, Security Program, and System Life Cycle Security.

Vulnerability — a flaw or weakness that may allow harm to occur to an IT system or activity.

APPENDIX D

APPENDIX D — SELECTED GOVERNMENT IT SECURITY REFERENCES

Federal Laws and Regulations

Privacy Act of 1974, Public Law 93-579

Computer Fraud & Abuse Act of 1986, as amended, Public Law 99-474

Computer Security Act of 1987, Public Law 100-235

Paperwork Reduction Act of 1978, as amended in 1995, U.S. Code 44 Chapter 35

Freedom of Information Act of 1974, 5 U.S. Code Section 552

OMB Circular A-123, *Internal Control Systems*

OMB Circular A-127, *Financial Management Systems*

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Federal Information Processing Standards

FIPS Publication 31, *Guidelines for ADP Physical Security and Risk Management*

FIPS Publication 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*

FIPS Publication 46-2, *Data Encryption Standard*

FIPS Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*

FIPS Publication 73, *Guidelines for Security of Computer Applications*

FIPS Publication 74, *Guidelines for Implementing and Using the NIST Data Encryption Standard*

FIPS Publication 81, *DES Modes of Operation*

FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control*

FIPS Publication 87, *Guidelines for ADP Contingency Planning*

FIPS Publication 88, *Guideline on Integrity Assurance and Control in Database Administration*

FIPS Publication 102, *Guideline for Computer Security Certification and Accreditation*

FIPS Publication 112, *Standard on Password Usage*

FIPS Publication 113, *Standard on Computer Data Authentication*

FIPS Publication 139, *Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications*

FIPS Publication 140-1, *Security Requirements for Cryptographic Modules*

FIPS Publication 141, *Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment*

FIPS Publication 171, *Key Management Using ANSI X9.17*

FIPS Publication 180-1, *Secure Hash Standard*

FIPS Publication 181, *Automated Password Generator*

FIPS Publication 185, *Escrowed Encryption Standard*

FIPS Publication 186, *Digital Signature Standard*

FIPS Publication 188, *Standard Security Label for Information Transfer*

FIPS Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*

FIPS Publication 191, *Guideline for the Analysis of Local Area Network Security*

Selected NIST Special Publications

SP 500-120, *Security of Personal Computer Systems*

SP 500-133, *Technology Assessment: Methods for Measuring the Level of Computer Security*

SP 500-134, *Guide on Selecting ADP Backup Process Alternatives*

SP 500-153, *Guide to Auditing for Controls and Security: A System Development Life Cycle Approach*

SP 500-156, *Message Authentication Code (MAC) Validation System: Requirements and Procedures*

SP 500-157, *Smart Card Technology: New Methods for Computer Access Control*

SP 500-166, *Computer Viruses and Related Threats: A Management Guide*

SP 500-172, *Computer Security Training Guidelines*

SP 800-2, *Public-Key Cryptography*

SP 800-3, *Establishing a Computer Security Incident Response Capability*

SP 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*

SP 800-5, *A Guide to the Selection of Anti-Virus Tools and Techniques*

SP 800-6, *Automated Tools for Testing Computer System Vulnerability*

SP 800-7, *Security In Open Systems*

SP 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*

SP 800-10, *Keeping Your Site Comfortably Secure: An Introducement to Internet Firewalls*

SP 800-12, *An Introduction to Computer Security: The NIST Handbook*

SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*

NISTIR 4749, *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out*

NISTIR 4939, *Threat Assessment of Malicious Code and External Attacks*

Note: Some of these documents can be found on the NIST ITL Computer Security Division's Computer Security Resource Clearinghouse - CSRC - at:

http://csrc.nist.gov/publications/

Older documents that are not available on CSRC can be obtained by calling the National Technical Information Service at (703) 605-6000, or 1-800-553-NTIS (6847), or by writing:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161