Information technology (IT) security is "a new high-risk area that touches virtually every major aspect of government
operations," according to a recent U.S. General Accounting Office (GAO) report on federal government information
technology systems. GAO cited several factors that contributed to the risks, including insufficient awareness and
understanding of information security risks on the part of managers, and a shortage of personnel with sufficient technical
expertise needed to manage security controls.

Organizations are challenged to provide their staff members with the appropriate awareness, training, and education to
enable them to carry out their responsibilities effectively and to protect the organization's information technology
systems. This bulletin introduces some of the principles for the training of staff members according to their roles within
their organizations and for measuring the results of the training. The material in this bulletin was excerpted from NIST
Special Publication 800-16, Information Technology Security Training Requirements: A Role- and
Performance-Based Model. The document was developed by the Federal Computer Security Program Managers
Forum and the Federal Information Systems Security Educators' Association (FISSEA). The guideline is available in
paper copy from the Government Printing Office and in electronic format from NIST's Web pages:
   http://csrc.nist.gov/nistpubs/.

Background

Staff members play a critical role in protecting the integrity, confidentiality, and availability of information of their
organizations' information technology systems and networks. The Computer Security Act of 1987 (Public Law 100-235)
established requirements for "the mandatory periodic training in computer security awareness and accepted computer
practices of all employees who are involved with the management, use, or operation of each Federal computer system
within or under the supervision of that agency."

To implement this provision of the Computer Security Act, the National Institute of Standards and Technology (NIST)
worked with the U.S. Office of Personnel Management (OPM) to develop the first training guidelines, which were
issued in November 1989 (NIST Special Publication 500-172, Computer Security Training Guidelines). In January
1992, OPM revised the federal personnel regulations to mandate that agencies provide training. In 5 CFR Part 930,
Employees Responsible for the Management or Use of Federal Computer Systems, agencies are directed to provide
mandatory training for current and new employees. Training is also required whenever there is a significant change in the
agency's IT security environment or procedures, or when an employee enters a new position that involves sensitive
information. Further, periodic refresher training should be provided, based on the sensitivity of the information the
employee handles. Office of Management and Budget (OMB) Circular A-130, "Management of Federal

Information
Resources," Appendix III, "Security of Federal Automated Information Resources," reinforces these agency
responsibilities for providing mandatory training, including specialized training based on staff members' IT security
responsibilities.

Special Publication (SP) 500-172 provided a framework for determining the training needs of particular categories of
employees (including contractors) involved with sensitive but unclassified computer systems, but it was oriented to the
mainframe environment of its time. SP 800-16 supersedes SP 500-172 and provides a new conceptual framework for IT
security training that is appropriate to today's distributed computing environment. It is expected that the framework will
be extended in the future to accommodate changing technologies and their related risk management decisions.

Principles of the New Approach to Results-Based Learning

Results-based learning focuses on the job functions that individuals perform, and on their specific roles and
responsibilities, rather than on their job titles. This approach to learning recognizes that individuals have unique
backgrounds and different levels of understanding. Also individuals may have more than one organizational role, and
will need security training that satisfies the specific responsibilities of each role.

Everyone needs basic training in IT security concepts and procedures. After the basic training, three levels of IT security
training are recommended - beginning, intermediate, and advanced training. Each level of training is linked to roles and
responsibilities. Because individuals may perform more than one role within the organization, they may need intermediate
or advanced level IT security training in their primary job role, but only the beginning level in a secondary or tertiary role.
Thus training can be tailored to individual employee needs and career mobility, and to an organization's evolving or
changing mission and its mix of job functions.

The results-based model for training provides an integrated framework to identify training needs throughout the
workforce and to ensure that everyone receives appropriate training. By relating job function to required IT security
knowledge, managers can identify the training needed to fulfill their IT security responsibilities, to understand the
consequences of denying or deferring training, and to plan and schedule training according to organizational priorities.

The results-based model also helps course developers identify the learning outcomes expected for individuals in various
roles with varying responsibilities. This facilitates the development of IT security course material targeted to the needs of
the federal workforce and encourages the development of basic training modules that can be readily customized or

adapted to an organization's needs.

Role-Based Model for Training

The model is based on the premise that learning is a continuum that starts with awareness, builds to training, and evolves
into education. While learning is a continuum in terms of levels of knowledge, the acquisition or delivery of that
knowledge need not proceed sequentially. Given resource constraints, organizations have a responsibility to evaluate the
scope of their IT security training needs and the effectiveness of the training provided in order to allocate future training
resources and to derive the greatest value or return on investment.

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. The model is used to identify the knowledge, skills,
and abilities an individual needs to perform the IT security responsibilities specific to their role in the organization. The
type of learning that individuals need becomes more comprehensive as they perform more complex multi-disciplinary
activities.

Awareness, Training, and Education

Awareness, training and education are all important processes for helping staff members carry out their roles and
responsibilities for information technology security, but they are not the same.

Awareness programs which have been established by many organizations are a prerequisite to IT security training.
Awareness presentations focus attention on security, and allow individuals to recognize IT security concerns. In
awareness activities, the learner is a recipient of information. Awareness relies on reaching broad audiences with
attractive packaging techniques. Examples of IT security awareness materials are promotional trinkets with motivational
slogans, videotapes, and posters or flyers.

Awareness presentations must be ongoing, creative, and motivational, with the objective of focusing the learner's
attention so that the learning will be incorporated into conscious decision-making. Learning achieved through a single
awareness activity tends to be short-term, immediate, and specific.

Detailed guidance on IT security awareness is outside the scope of the training guidelines. The fundamental value of IT
security awareness programs is that they set the stage for training by bringing about a change in attitudes which change
the organizational culture. The cultural change is the realization that IT security is critical because a security failure has
potentially adverse consequences for everyone.

Training addresses the needed security skills and competencies of practitioners of functional specialties other than IT
security. This includes managers, systems designers and developers, and acquisition and auditing staff members.
Training is more formal and more active than awareness activities and is directed toward building knowledge and skills to
facilitate job performance. IT security training encompasses IT security basics and literacy, and is tied to the individuals'
specific roles and responsibilities.

The IT security basics and literacy involve the generic concepts, terms, and associated learning modules that are common
among different groups of employees or organizations. In the federal government, this approach eliminates redundancies
and establishes a baseline of IT security knowledge for employees who may change jobs or organizations and use
different IT systems.

Education is another learning level beyond training and is usually limited to an organization's designated IT security
specialists. Providing formal education to this group is outside the purview of most federal agency training programs,
with some notable exceptions among national security-related agencies. Education (as distinguished from training) and
associated on-the-job experience are essential for IT security specialists to be able to fulfill their roles in an effective
manner.

Education integrates all of the security skills and competencies of the various functional specialties into a common body
of knowledge, adds a multi-disciplinary study of concepts, issues, and principles (technological and social), and strives
to produce IT security specialists and professionals capable of vision and responsiveness.

Formal education has become a key element to IT security. In the past, computer security specialists were practitioners
who came from the ranks of computer specialists. Security responsibilities were often assigned as collateral duties to their
primary functional specialty. Some federal agencies paid for occasional training courses for their designated Computer
Security Officers or specialists, but few agency officials recognized a need to enroll these critical staff members in formal
computer security educational programs. Agencies seldom required evidence of qualification or certification as a
condition of appointment.

IT security functions have become increasingly technologically and managerially complex and organizations are seeking
educated IT security professionals who can solve severe security and privacy problems and who can integrate security
principles with changing technology and evolving security implications.

Awareness is the point-of-entry for all employees into the progression of IT security knowledge levels. Training starts
with Security Basics and Literacy, and then builds a wide range of security-related skills needed by

employees.

Education is the capstone of the learning continuum, creating expertise necessary for IT security specialists and
professionals.

Learning Styles and Teaching Methods

Providing training to individuals does not necessarily ensure that learning has occurred. Learning can best be
demonstrated by subsequent on-the-job performance. The guideline describes learning objectives that are
performance-based, rather than content-based, and that provide benchmarks for evaluating learning effectiveness. This
enables evaluation to become a component of organizational IT security training programs and provides an evaluation
planning process.

Individuals learn in different ways, and each has a preferred or primary learning style. The learning approach most
effective for individuals is a function of their preferred learning style, education, and prior experience. In learning
information or concepts, some students will do better through reading; others prefer to listen to a lecture; still others need
to participate in a discussion in order to understand the material.

Instructors should be aware of these learning style differences and should use a variety of teaching approaches and
presentation formats such as multimedia, searchable databases, text, graphics, simulations, team teaching, decision trees,
and interactive learning. A variety of delivery approaches can be used including classroom instruction, computer-based
instruction, manuals, self-paced instruction books, videotapes, interactive workshops with "hands-on" exercises, and
one-on-one mentoring/coaching by senior staff.

Materials developers and trainers should consider the education and experience of their target audience and tailor their
presentation approach and content accordingly. An individual with an advanced degree will perceive and learn new
material in a manner that is different from an individual without a degree but who has extensive on-the-job experience.

Adult learners learn best when they perceive the relevance of the knowledge or skill to their current job or to their career
advancement. When the instructor is able to emphasize the applicability and practical purpose of the material to be
mastered, the learning retention rates and the subsequent transference of the new knowledge or skill to the learners' jobs
and organizational settings will be enhanced.