Building an Information Technology Security Awareness and Training Program

Recommendations of the National Institute of Standards and Technology

Mark Wilson and Joan Hash
Building an Information Technology Security Awareness and Training Program

Recommendations of the National Institute of Standards and Technology

Mark Wilson and Joan Hash

COMPUTER SECURITY

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Draft: July, 2002
Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL’s research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.
Table of Contents

ACKNOWLEDGEMENTS ............................................................................................................. V

EXECUTIVE SUMMARY ............................................................................................................. VI

1. INTRODUCTION ..................................................................................................................... 1

1.1 PURPOSE ............................................................................................................................ 1

1.2 SCOPE .................................................................................................................................. 1

1.3 POLICY .................................................................................................................................. 2

1.4 ROLES AND RESPONSIBILITIES ....................................................................................... 3

1.4.1 AGENCY HEAD .............................................................................................................. 3

1.4.2 CHIEF INFORMATION OFFICER .................................................................................... 4

1.4.3 INFORMATION SYSTEMS SECURITY OFFICER (ISSO) ............................................. 4

1.4.4 MANAGERS .................................................................................................................... 4

1.4.5 USERS ............................................................................................................................ 5

2. COMPONENTS: AWARENESS, TRAINING, EDUCATION .................................................. 6

2.1 “THE CONTINUUM” .......................................................................................................... 6

2.2 AWARENESS ..................................................................................................................... 7

2.3 TRAINING .......................................................................................................................... 8

2.4 EDUCATION ...................................................................................................................... 8

2.5 PROFESSIONAL DEVELOPMENT ..................................................................................... 9

3. BUILDING A STRATEGY ....................................................................................................... 10

3.1 DETERMINING AGENCY AWARENESS AND TRAINING NEEDS .................................. 10

3.2 CONDUCTING A NEEDS ASSESSMENT ........................................................................ 15

3.3 DEVELOPING AN AWARENESS AND TRAINING STRATEGY AND PLAN .................. 18

3.4 ESTABLISHING PRIORITIES ............................................................................................ 19
3.5 SETTING THE BAR..................................................................................................................20

4. DEVELOPING AWARENESS AND TRAINING MATERIAL ........................................22
4.1 DEVELOPING AWARENESS MATERIAL ........................................................................22
   4.1.1 SELECTING AWARENESS TOPICS................................................................................22
   4.1.2 SOURCES OF AWARENESS MATERIAL .....................................................................24
4.2 DEVELOPING TRAINING MATERIAL ..............................................................................24
   4.2.1 A MODEL FOR BUILDING TRAINING COURSES: NIST SPECIAL PUB. 800-16 .25
   4.2.2 SOURCES OF TRAINING COURSES AND MATERIAL ..............................................27

5. IMPLEMENTING THE AWARENESS AND TRAINING PROGRAM .........29
5.1 COMMUNICATING THE PLAN .......................................................................................29
5.2 TECHNIQUES FOR DELIVERING AWARENESS MATERIAL ....................................31
5.3 TECHNIQUES FOR DELIVERING TRAINING MATERIAL .............................................32

6. POST-IMPLEMENTATION .................................................................................................33
6.1 MONITORING SUCCESS ..............................................................................................33
6.2 EVALUATION AND FEEDBACK ..................................................................................35
6.3 MANAGING CHANGE ..................................................................................................36
6.4 ONGOING IMPROVEMENT ("RAISING THE BAR") ....................................................37
6.5 PROGRAM SUCCESS INDICATORS .............................................................................38
Acknowledgements

We would like to express our thanks to George Bieber, Department of Defense; Carolyn Schmidt, NIST IT Security Office; Jaren Doherty, National Institutes of Health (NIH); Becky Vasvarya, National Oceanographic and Atmospheric Administration (NOAA); Richard Stone, Internal Revenue Service (IRS); and Pauline Bowen, Richard Kissel, and Tanya Brewer-Joneas of NIST. We would also like to thank the NIST Technical Editor, Elizabeth Lennon, for her efforts editing this document.

Noteworthy contributions were also made by Ann L. Brown, Department of Health and Human Services (DHHS) Indian Health Service; Carolyn O’Connor, DHHS/Program Support Center (PSC); and to Charles A. Filius, DHHS/PSC.

Finally, we wish to thank the members of the Executive Board of the Federal Information Systems Security Educators’ Association (FISSEA) - Barbara Cuffie, Social Security Administration (SSA); Patricia Black, Treasury Department; and Dara Murray, DHHS/PSC.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.
Executive Summary

NIST Special Publication 800-50, *Building An Information Technology Security Awareness and Training Program*, provides guidance for putting (in place) an effective information technology (IT) security program and supports requirements specified in the Office of Management and Budget (OMB) Circular A-130, Appendix III. The guidelines provided here are not mandatory but need to be considered in the context of specific agency organizational and operational requirements. A strong IT security program cannot be put in place without significant attention given to training agency employees on security policy and techniques. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk since security of agency resources is as much a human issue as it is a technology issue.

Everyone has a role to play in the success of a security training program but key responsibility to ensure that an effective program is established agency-wide lies with agency heads, Chief Information Officers (CIOs), and Security Program Managers. Scope and content of the program must be tied to existing security directives and established agency security policy.

The document identifies four steps in designing and implementing a security training and awareness program.

- **Designing an Awareness and Training Program:** In this step, an agency-wide needs assessment is conducted and a training strategy developed and approved. This strategic planning document identifies implementation tasks to be performed, in support of established agency security training goals.

- **Developing Awareness and Training Material:** This step focuses on available training sources, scope, content, and development of training material including solicitation of contractor assistance if needed.

- **Program Implementation:** This step addresses effective communication and roll out of the awareness and training program. It also addresses options for delivery of awareness and training material (web-based, distance learning, video, on-site, etc.).

- **Post-Implementation:** This step gives guidance on keeping the program current and monitoring its effectiveness. Effective feedback methods are described (surveys, focus groups, benchmarking, etc.).

The document also discusses three common models used in managing a security training function.
• **Centralized**: All responsibility resides with a central authority (CIO/ISSO).

• **Partially Decentralized**: Training policy and strategy lie with a central authority, but implementation responsibilities are distributed.

• **Decentralized**: Only policy development resides with a central authority and all other responsibilities are delegated to individual agency components.

The type of model considered should be based on budget and resource allocation assessments.
1. Introduction
Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands their responsibilities. As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. It is also understood that the “people factor” - not technology - is the key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this “asset.” A robust and entity-wide awareness and training program is the key to ensuring that people understand their IT security responsibilities, and understand that they will be held accountable for the proper use and protection of IT resources entrusted to them.

1.1 Purpose
This document provides guidelines for building and maintaining a comprehensive awareness and training program, as part of an organization’s IT security program. The guidance is presented in a life-cycle approach, ranging from designing, developing, and implementing an awareness and training program, through post-implementation of the program. The document includes guidance on how IT security professionals can identify awareness and training needs, develop a training plan, and get organizational buy-in for the awareness and training program efforts. The guidance also describes how to:

• Select awareness and training topics;
• Find sources of awareness and training material;
• Implement awareness and training material, using a variety of methods;
• Evaluate the success of the program; and
• Update and improve the focus as technology and organizational focus change.

1.2 Scope
The scope of this guidance covers what an organization should do to design, develop (material), implement, and maintain an IT security awareness and training program, as a part of the IT security program. The scope includes awareness and training needs of all employees of an organization, from users to supervisors and functional managers to executive-level managers. The guidance also discusses professional development (professionalization) and certification issues - topics that continue to gain acceptance in organizations. This document mentions and defines IT security education, but does not address it in-depth, since it generally applies only to the IT security program manager and staff.
1.3 Policy

The Computer Security Act of 1987 states, “Each agency shall provide 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.” OMB Circular A-130, Appendix III, addresses training as an element of a system security plan for a general support system and as an element of an application security plan for a major application. Regarding the training element of a system security plan, the Circular states, “Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall ensure that employees are versed in the rules of the system . . . and apprise them about available technical assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.” The Circular states that as part of an application security plan, “Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).”

Additionally, the Government Information Security Reform Act (GISRA) of 2000 tasks the head of each agency with the responsibility to “ensure that the agency has trained personnel sufficient to assist the agency in complying with (these requirements) and related policies, procedures, standards, and guidelines.” GISRA also requires that the head of each agency “delegate to the agency Chief Information Officer (CIO) (or a comparable official), the authority to administer . . . training and overseeing personnel with significant responsibilities for information security . . .” GISRA also states that the required “agencywide information security program” shall include “security awareness training to inform personnel of:

- (i) information security risks associated with the activities of personnel, and
- (ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks.”

The reporting instructions for the GISRA Act, dated (get date), requires that agencies:

- Describe the specific measures of performance used by the agency to ensure that the agency CIO ensures the training of agency employees with significant security responsibilities; and
- Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Agencies also need to identify the total number of agency
employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.

1.4 Roles and Responsibilities
While it is important to understand the policies that require agencies to develop and implement awareness and training, it is crucial that agencies understand who has responsibility for IT security awareness and training. This section identifies the audiences for which this document is written, and identifies and describes those within an organization that have responsibility for IT security awareness and training.

This guidance is intended to be useful to several key audiences in an organization, including, but not limited to: the CIO, the information systems security officer (ISSO) and staff, managers and their contractors, and agency training coordinators. (The terms “information systems security officer” and “security program manager” will be used interchangeably in this document.) The success of an organization’s awareness and training program, and that of the overall IT security program, depends on the ability of these people to work toward a common goal of protecting the organization’s information and IT-related resources.

Some organizations have a mature IT security program, while other organizations may be struggling to achieve basic staffing, funding, and support. The form that an awareness and training program takes from agency to agency can vary greatly. This is due, in part, to the maturity of that program. (Differences in organizational culture are indicated by the placement of the IT security program, funding support, access to and support by management.) (See Section 3.1 for examples of different awareness and training program models that can be implemented in an agency.)

1.4.1 Agency Head
Agency heads must ensure that high priority is given to effective security awareness and training for the workforce. This includes implementation of a viable IT security program with a strong awareness and training component. Agency heads should:

- Designate a CIO;
- Assign responsibility for IT security;
- Ensure that an agency-wide IT security program is implemented, is effective, is well-supported by resources and budget; and
- Ensure that the agency has trained personnel sufficient to protect its IT resources.
1.4.2 Chief Information Officer
Chief Information Officers (CIOs) are tasked by the GISRA to administer training and overseeing personnel with significant responsibilities for information security. CIOs should work with the agency ISSO and program managers to:

- Establish overall strategy for the IT security awareness and training program;
- Ensure that the agency’s IT security awareness and training program is funded;
- Ensure the training of agency personnel with significant security responsibilities;
- Ensure that all employees are sufficiently trained in their security responsibilities; and
- Ensure that effective tracking and reporting mechanisms are in place.

1.4.3 Information Systems Security Officer (ISSO)
The ISSO has tactical-level responsibility for the awareness and training program. In this role, the ISSO should:

- Ensure that awareness and training material developed is appropriate and timely for the intended audience;
- Ensure that awareness and training material is deployed using effective means to reach the intended audience;
- Ensure that employees and managers have an effective way to provide feedback on the awareness and training material and its presentation;
- Ensure that awareness and training material is reviewed periodically and updated when necessary; and
- Assist in establishing a tracking and reporting strategy.

1.4.4 Managers
Managers have responsibility for complying with IT security awareness and training requirements established for their employees. Managers should:

- Work to reduce errors and omissions by users;
- Work with the CIO and ISSO to meet these shared responsibilities;
- Serve in the role of system owner and/or data owner, where applicable; and
• Ensure that all users of their systems (e.g., general support systems and applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access, and that users understand specific rules of the system. 

This includes contractors if some activities are outsourced.

1.4.5 Users

Users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and IT vulnerabilities. Users must:

• Understand and comply with agency security policy;

• Be appropriately trained in the rules of behavior for the systems and applications to which they have access;

• Work with management to meet training needs; and

• Be aware of actions they can take to better protect their agency’s information. These actions include, but not be limited to proper password usage, data backup, proper anti-virus protection, and following rules established to avoid social engineering attacks (the surreptitious or stealthy practice of gaining unauthorized access to systems or networks by posing as one who does or should have access).
2. **Components: Awareness, Training, Education**

Security awareness and training should not solely be focused on the organization’s employees. Management should set the example for proper IT security behavior within an organization. An awareness program should begin with an effort that can be deployed and implemented in various ways and is aimed at all levels of the organization including senior and executive managers. The effectiveness of this effort will usually determine the effectiveness of the awareness and training program. This is also true for a successful computer security program.

A successful IT security program consists of: 1) developing IT security policy that reflects business needs tempered by known risks; 2) informing employees of their IT security responsibilities, as documented in agency security policy; and 3) establishing processes for monitoring and reviewing the program.

An awareness and training program is crucial in that it is the vehicle for disseminating information that employees, including managers, need in order to do their jobs. In the case of a computer security program, it is the vehicle to be used to communicate security requirements across the enterprise.

An effective IT security awareness and training program explains proper rules of behavior for the use of agency IT systems and information. It communicates IT security policies and procedures that need to be followed. This must precede and lay the basis for any sanctions imposed due to noncompliance. Users first should be informed of the expectations. Accountability must be derived from a fully informed, well-trained, and aware workforce.

This section describes the relationship between awareness, training, and education – the awareness-training-education continuum.

2.1 **“The Continuum”**

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The continuum is further described in Chapter 2 of NIST Special Publication 800-16 – “Information Technology Security Training Requirements: A Role- and Performance-Based Model,” available at http://csrc.nist.gov.
2.2 Awareness

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in NIST Special Publication 800-16 as follows:

“Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.”
Training strives to produce relevant and needed security skills and competencies. An example of a topic for an awareness session (or awareness material to be distributed) is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user’s system, what the user should do to protect the system, and what the user should do if a virus is discovered. A list of possible awareness topics can be found in Section 4.1.1.

A bridge or transitional stage between awareness and training consists of what NIST Special Publication 800-16 calls “Security Basics and Literacy.” The basics and literacy material is a core set of terms, topics, and concepts. Once an organization has established a program that increases the general level of security awareness and vigilance, the basics and literacy material allows for the development or evolution of a more robust awareness program. It also provides the foundation for the training program.

### 2.3 Training

Training is defined in NIST Special Publication 800-16 as follows: “The ‘Training’ level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing).” The most significant difference between training and awareness is that training seeks to teach skills to allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues. The skills acquired during training are built upon the awareness foundation, in particular, upon the security basics and literacy material. A training curriculum need not necessarily lead to a formal degree from an institution of higher learning. However, a training course may contain much of the same material that is found in a course that a college or university includes in a certificate or degree program.

An example of training is an IT security course for system administrators, which should address in detail the management controls, operational controls, and technical controls that should be implemented. Management controls include policy, IT security program management, risk management, and life cycle security. Operational controls include personnel and user issues, contingency planning, incident handling, awareness and training, computer support and operations, and physical and environmental security issues. Technical controls include identification and authentication, logical access controls, audit trails, and cryptography. (See NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, for in-depth discussion of these controls.)

### 2.4 Education

Education is defined in NIST Special Publication 800-16 as follows: “The ‘Education’ level 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
Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge . . . and strives to produce IT security specialists and professionals capable of vision and pro-active response."

An example of education is a degree program at a college or university. However, some people take a course or several courses to develop or enhance their skills in a particular discipline. This is training as opposed to education. Many colleges and universities offer certificate programs, wherein a student may take two, six, or eight classes, for example, in a related discipline, and is awarded a certificate upon completion. Often, these certificate programs are conducted as a joint effort between schools and software or hardware vendors. These programs are more characteristic of training than education. Drawing a clear line between education and training has become more difficult. Those responsible for security training need to assess both types of programs and decide which one better addresses identified needs.

2.5 Professional Development

Another type of learning is the professional development of an IT security professional. While the education portion of the continuum includes the “education and experience of the IT security specialists and professionals,” professional development – in the form of studying for tests that lead to professional certification – is generally thought to be training. The preparatory work to testing for such a certification normally includes study of a prescribed body of knowledge or curriculum completed with on-the-job experience. The movement toward professionalization within the IT security field can be seen among IT security officers, IT security auditors, and system/network administrators.
3. Building A Strategy

There are three major steps in the development of an IT security awareness and training program – designing the program (including the strategy to which the material can be built), developing the material, and implementing the program. Even a small amount of IT security awareness and training can go a long way toward improving the IT security posture of, and vigilance within, an organization. This section describes the first step of designing an awareness and training program: building a strategy.

Awareness and training programs must be designed with the organization mission in mind. It is important that the awareness and training program strategy support the business needs of the organization and be relevant to the organization’s culture and IT architecture. The most successful programs are those where users feel relevancy to the subject matter and issues presented.

Designing an IT security awareness and training program answers the question “What is our strategy for developing and implementing awareness and training opportunities which are compliant with existing directives?” The strategy identifies and incorporates the agency’s awareness and training needs, seeks organizational buy-in, and culminates in development of an effective agency-wide awareness and training plan.

This section will describe:

- How to structure the awareness and training activity;
- How to conduct a needs assessment;
- How to develop an overall strategy based on results of the assessment;
- How to establish priorities; and
- How to “set the bar” (the complexity of the material) properly.

3.1 Determining Agency Awareness and Training Needs

An awareness and training program may be designed, developed, and implemented in many different ways. Three common approaches or models are described below:

- Model 1: Centralized policy, strategy, and implementation;
- Model 2: Centralized policy and strategy, distributed implementation; and
- Model 3: Centralized policy, distributed strategy, and implementation.
The model that is embraced and established to oversee the awareness and training program activity is dependent on:

- The size of the organization;
- Defined organizational roles and responsibilities; and
- Budget allocations and authority.

**Model 1: Centralized Program Management Model (Centralized Policy, Strategy, and Implementation)**

In this model, responsibility and budget for the entire organization’s IT security awareness and training program is given to a central authority. All directives, strategy development, planning, and scheduling is coordinated through this “security awareness and training” authority.

Since the awareness and training strategy is developed at the central authority, the needs assessment – which helps determine the strategy – is also conducted by the central authority. The central authority also develops the training plan as well as the awareness and training material. The method(s) of implementing the material throughout the organization is determined and accomplished by the central authority. Typically, in such an organization, both the CIO and ISSO are organizationally located within this central authority.
Communication between the central authority and the organizational units travels in both directions. The central authority communicates the agency’s policy directives regarding IT security awareness and training, the strategy for conducting the program, and the material and method(s) of implementation to the organizational units. The organizational units provide information requested by the central authority. For example, to meet its GISRA responsibilities, the central authority may collect data on the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit can also provide feedback on the effectiveness of awareness and training material and on the appropriateness of the method(s) used to implement the material. This allows the central authority to fine-tune, add or delete material, or modify the implementation method(s).

This centralized program management model is often deployed by agencies which:

- Are relatively small or which have a high degree of structure and central management of most IT functions;
- Have, at the headquarters level, the necessary resources, expertise, and knowledge of the mission(s) and operations at the unit level; or
- Have a high degree of similarity in mission and operational objectives across all of its components.

Model 2: Partially Decentralized Program Management Model (Centralized Policy and Strategy; Distributed Implementation)

In this model, security awareness and training policy and strategy are defined by a central authority, but implementation is handed off to line management officials in the organization. Awareness and training budget allocation, material development, and scheduling are their responsibility.

The needs assessment is conducted by the central authority, since they still determine the strategy for the awareness and training program. Policy, strategy, and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their awareness and training material, and determine the method(s) of deploying the material within their own units.

As was the case in the centralized program management model (Model 1), communication between the central authority and the organizational units also travels in both directions in this model. The central authority communicates the agency’s policy directives regarding IT security awareness and training, the strategy for conducting the program, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for developing training plans and for implementing the program, and may provide guidance or training to the organizational units so that they can carry out their responsibilities.
The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status of unit training plans, and progress reports on the status of implementing the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions. The organizational unit may be asked to provide lessons learned, so the central authority can provide effective guidance to other units.

This partially decentralized program management model is often deployed by agencies which:

- Are relatively large or which have a fairly decentralized structure with clear responsibilities assigned to both the headquarters (central) and unit levels;

- Have functions which are spread over a wide geographical area; or

- Have organizational units with diverse missions, such that awareness and training programs may differ significantly, based on unit-specific needs.
Model 3: Decentralized Program Management Model (Centralized Policy; Distributed Strategy and Implementation)

In this model, the central security awareness and training authority (CIO/ISSO) disseminates broad policy and expectations regarding security awareness and training requirements, but gives responsibility for executing the entire program to other organizational units. This model normally uses a series of distributed authority directives, driven from the central authority. This normally means creation of a subsystem of CIOs and ISSOs subordinate to the central CIO and ISSO.

*Figure 3-3: Model 3 – Decentralized Program Management*

The needs assessment is conducted by each organizational unit, since in this model, the units determine the strategy for the awareness and training program. Policy and budget are passed from the central authority to the organizational units. Based on the strategy, the organizational units develop their own training plans. The organizational units develop their awareness and training material, and determine the method(s) of deploying the material within their own units.

As was the case in the centralized program management model (Model 1) and the partially decentralized program management model (Model 2), communication between the central authority and the organizational units travels in both directions in this model. The central authority communicates the agency’s policy directives regarding IT security awareness and training, and the budget for each organizational unit. The central authority may also advise the organizational units that they are responsible for conducting their
own needs assessment, developing their strategy, developing training plans, and implementing the program. The central authority may provide guidance or training to the organizational units so that they can carry out their responsibilities.

The central authority may require periodic input from each organizational unit, reporting the budget expenditures made, the status and results of needs assessments, the strategy chosen by the organizational unit, the status of training plans, and progress reports on the implementation the awareness and training material. The central authority may also require the organizational units to report the number of attendees at awareness sessions, the number of people trained on a particular topic, and the number of people yet to attend awareness and training sessions.

This decentralized program management model is often deployed by agencies which:

- Are relatively large;
- Have a very decentralized structure with general responsibilities assigned to the headquarters (central) and specific responsibilities assigned to unit levels;
- Have functions which are spread over a wide geographical area; or
- Have quasi-autonomous organizational units with separate and distinct missions, such that awareness and training programs may need to differ greatly.

Once the model to be employed is identified, the approach to conducting a needs assessment should be defined consistent with the organizational models.

### 3.2 Conducting a Needs Assessment

A needs assessment is a process that can be used to determine an organization’s awareness and training needs. The results of a needs assessment can provide justification to convince management to allocate adequate resources to meet those awareness and training needs.

In conducting a needs assessment, it is important that key personnel be involved. As a minimum, the following roles should be addressed in terms of any special training needs:

- Executive Management – Organizational leaders need to fully understand directives and laws that form the basis for the security program. They also need to comprehend their leadership roles in ensuring full compliance by employees within their units.
• Key Security Personnel (security program managers and security officers) – These individuals act as expert consultants for their organization and therefore must be well educated on security policy and accepted best practices.

• System Owners – Must have a broad understanding of security policy and a high degree of understanding regarding security controls and requirements applicable to systems they manage.

• System Administrators and Key IT Support Personnel – These are individuals entrusted with a high degree of authority over trusted support operations critical to a successful security program. They need a higher degree of technical knowledge in effective security practices and implementation.

• Operational Managers and System Users – Need a high degree of security awareness and training on security controls and rules of behavior for systems they use to conduct business operations.

A number of sources of information in an agency can be used to determine IT security awareness and training needs, and a number of ways exist to collect that information. Figure 3-4 suggests techniques for gathering information as part of a needs assessment. Appendix A contains a sample needs assessment interview and questionnaire.

- Interviews with all key groups and organizations identified
- Organizational surveys
- Review and assessment of available resource material, such as current awareness and training material, training schedules, and lists of attendees
- Review of any findings and/or recommendations from oversight bodies (e.g., Congressional inquiry, inspector general, internal review/audit, and internal controls program) or program reviews regarding the IT security program
- Conversations and interviews with management, owners of general support systems and major applications, and other organization staff whose business functions rely on IT
- Analysis of events, including denial of service attacks, website defacements, hijacking of systems used in subsequent attacks, successful virus attacks, might indicate the need for training of specific groups of people
- The study of trends first identified in industry, academic, or government publications or by training/education organizations. The use of these “early warning systems” can provide insight into an issue within the organization that has yet to be seen as a problem.

**Figure 3-4: Techniques for Gathering Information as Part of a Needs Assessment**
Figure 3-5 illustrates overarching agency-specific issues that must be understood at the start of the needs assessment. The techniques shown in Figure 3-4 should provide information that offers insight into, and understanding of, these issues. These issues should feed necessary information into the needs assessment process. Understanding them will help shape the strategy and design of the IT security awareness and training program.

![Diagram](image)

**Figure 3-5: Understanding Overarching Agency-Specific Issues**

Analysis of the information gathered should provide answers to key questions, shown in Figure 3-6.

- What awareness, training, and/or education are needed (what is required)?
- What is currently being done to meet these needs?
- What is the current status regarding how these needs are being addressed (how well are current efforts working)?
- Where are the gaps between the needs and what is being done (what more needs to be done)?
- Which needs are most critical?

**Figure 3-6: Key Questions to be Answered in Performing a Needs Assessment**
Figure 3-7 shows the relationship between awareness and training requirements and current efforts. The shaded area represents the additional IT security awareness and/or training efforts that need to be made. The needs assessment can help identify these additional needs – the gap between what is currently being done and what is required.

### Assessed Level of Need

Assessed Level of Need

<table>
<thead>
<tr>
<th>Assessed Level of Need</th>
<th>Current Level of Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3-7: Required Awareness and Training Versus Current Effort**

Once the needs assessment has been completed, information necessary to develop a strategic security training plan (SSTP) is available. The SSTP should cover the entire organization and incorporate priorities identified by the needs assessment.

### 3.3 Developing an Awareness and Training Strategy and Plan

Completion of the needs assessment allows an agency to develop a strategy for implementing its IT security awareness and training program. The plan is the working document that contains the elements that make up the strategy. The plan should include and describe the following elements:

- Existing policy at the national and local level that requires the awareness and training to be accomplished;

- Roles and responsibilities of agency personnel who should design, develop, implement, and maintain the awareness and training material, and should ensure that the appropriate employees attend or view the applicable material;

- For awareness, training, education, and professional development (including certification), document for each aspect of the program:
• Goals – what is to be accomplished?
• Learning objectives – what training experiences help meet the goal?
• Topics to be addressed in each session or course – what specific course content?
• Deployment – how material will be presented or made available;
• Documentation, feedback, and evidence of learning – how the organization will track who has been trained and who needs training, how attendees can provide comments on the appropriateness of material, and how the agency will determine if the attendee benefits from exposure to the awareness or training material; and
• Evaluation – how the material is reviewed and updated.

The awareness and training plan should also clearly identify the frequency that employees should be exposed to awareness and training material. At a minimum, the entire workforce should be exposed to awareness material at least annually. A continuous awareness program, using various methods of delivery throughout the year, can be very effective. Security training for groups of employees with significant security responsibility (e.g., system and network administrators, managers, and security officers) should be incorporated into their functional training ongoing as needed.

Appendix B contains a sample awareness and training plan.

3.4 Establishing Priorities

Once the security awareness and training strategy and plan have been finalized, an implementation schedule must be established. If this needs to occur in phases due to budget constraints and resource availability, it is important to decide what factors you will use to influence your decision-making as to which initiative to schedule first and in what sequence. Key factors to consider are:

• Availability of Material/Resources – If awareness and training material are readily available and necessary resources on board, key initiatives in the plan can be scheduled early on. However, if course material development is necessary and/or instructor availability needs to be scheduled, then build these delays into your priority settings.

• Role and Organizational Impact – It is very common to address priority in terms of organizational role and risk. Broad-based awareness initiatives that are able to address the enterprise-wide mandate may receive very high priority because it assures that rules of good security practice are delivered to the workforce quickly. Also, it is very common to look at jobs in the organization that are “high trust”/”high impact” positions over the IT infrastructure (e.g., security program managers, security
officers, system administrators, security administrators, etc.) and ensure that they receive high priority in the roll-out strategy.

- **State of Current Compliance** – This involves looking at major gaps in the awareness and training program (e.g., gap analysis) and targeting deficient areas for early roll-out.

- **Critical Project Dependencies** – If there are projects dependent upon a segment of security training in order to prepare the necessary requirements for the system involved (e.g., Windows 2000, firewalls, VPNs), then the training schedule needs to ensure that the training occurs within the stipulated timeframe necessary to address these dependencies.

### 3.5 Setting the Bar

“Setting the bar” means that a decision must be made as to the complexity of the material that will be developed. The complexity must be commensurate with the role of the person who will undergo the learning effort. Material should be developed based on two important criteria: 1) the target audience’s position within the organization, and 2) knowledge of the security skills required for that position. The complexity of the material must be determined before development begins. Setting the bar applies to all three types of learning – awareness, training, and education.

When setting the bar for an awareness effort, the focus should be on the expected rules of behavior for using systems. These rules, which should come directly from agency policy, apply to everyone in the organization. As such, they should be explained clearly enough that there is no margin for confusion or misunderstanding. As an agency’s awareness program matures, and most employees have been exposed to the initial material, the bar can be raised. There are a number of ways to do this, including developing a basics and literacy course, following the guidance in Chapter 3 of the NIST Special Publication 800-16. Raising the bar will be further discussed in Section 6.

Setting the bar correctly is even more critical when developing training material. Since the goal of training is to produce relevant and needed skills and competencies, it is crucial that the needs assessment identify those individuals with significant IT security responsibilities, assess their functions, and identify their training needs. Training material should be developed that provides the skill set(s) necessary for the attendee to accomplish the security responsibilities associated with their job. IT security training material can be developed at a “beginning” level for a person who is just learning a discipline (e.g., system administrator, web or e-mail server administrator, auditor). Material can be developed at an “intermediate” level for someone who has more experience, and therefore more responsibility, in a discipline. “Advanced” material can be developed for those “centers of excellence” or agency subject matter experts whose jobs incorporate the highest level

---

Setting the bar means that a decision must be made as to the complexity of the material that will be developed; it applies to all three types of learning – awareness, training, and education.
of trust and an accompanying high level of IT security responsibility. Chapter 4 of NIST Special Publication 800-16 provides guidance on developing training material for these three levels of complexity, including learning objectives at each of the three levels to aid the training course developer.

Setting the bar for the education level of learning can be more difficult since curricula is developed by colleges and universities, and is impacted less in the short term by agency-specific needs. Once education needs have been identified within an organization – usually within the IT security office – a school that provides the needed learning can be found. An agency can “shop” for a local college or university whose certificate or degree program meets its needs or for a school that offers such a program through distance learning. As was the case with training material, a college or university should be selected because what it teaches meets the security needs of the agency personnel.
4. Developing Awareness and Training Material

Once the awareness and training strategy has been determined, supporting material can be developed. Material should be developed with the following in mind:

- **“What behavior do we want to reinforce?”** (awareness); and
- **“What skill or skills do we want the audience to learn and apply?”** (training).

In both cases, the focus should be on specific material that the audience should integrate into their job. To get and hold the audience’s attention, and more importantly, to inspire the audience to incorporate what they see or hear in a session, they need to feel that the material was developed specifically for them. Any presentation that “feels” canned – impersonal and so general as to apply to any audience – will be filed away as just another of the annual “we’re here because we have to be here” sessions. An awareness and training program can be effective if the material is interesting and current.

At some point the question will be asked – “Am I developing awareness or training material?” Generally, since the goal of awareness material is simply to focus attention on good security practices, the message that the awareness effort sends should be short and simple. The message can address one topic, or it can address a number of topics about which the audience should be aware.

The awareness audience must include all employees in an organization. This is because the message to be spread through an awareness program or campaign, by definition, should make all individuals aware of their commonly shared IT security responsibilities. On the other hand, the message in a training class is directed at a specific audience. The message in training material should include everything related to security that a particular audience needs to know in order to do their job. Training material is usually far more in-depth than is found in an awareness session or campaign.

4.1 Developing Awareness Material

The question to be answered when beginning to develop material for an organization-wide awareness program or campaign is, “What do we want all agency personnel to be aware of regarding IT security?” The awareness and training plan should contain a list of topics. E-mail advisories, online IT security daily news websites, and periodicals are good sources of ideas and material. Agency policy, program reviews, internal audits, internal controls program reviews, self-assessments, and spot-checks can also identify additional topics to address.

4.1.1 Selecting Awareness Topics

There are a significant number of topics that can be mentioned and briefly discussed in an awareness session or campaign. Topics can include, but are not limited to:
• Password usage/creation/changes
• Protection from viruses – scanning, updating definitions
• Policy – implications of non compliance
• Web usage – allowed vs. prohibited; monitoring
• Data backup and storage
• Incident response – contact whom? “What do I do?”
• Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
• Inventory and property transfer
• Personal use and gain issues – systems and work and home
• PDA security issues
• Laptop security while on travel
• Personally owned systems and software at work
• Software patches and security settings on client systems
• Software license restriction issues
• Supported/allowed software on organization systems
• Access control issues – least privilege and separation of duties
• Individual accountability – what this means in this organization
• Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
• Visitor control and physical access to spaces
• E-mail list etiquette – attached files and other rules
4.1.2 Sources of Awareness Material

In addition to numerous IT security awareness topics, there are a number of sources of material on these topics that can be incorporated into an awareness program. The material can address a specific issue, or in some cases, can describe how to begin to develop an entire awareness program, session, or campaign. Sources of timely material include, but are not limited to:

- E-mail advisories, issued by industry-hosted news groups, academic institutions, or the organization’s IT security office;
- Professional organizations and vendors;
- Online IT security daily news websites;
- Periodicals; and
- Conferences, seminars, and courses.

Awareness material can be developed using one theme at a time or by combining a number of themes or messages into a presentation. For example, a poster or a slogan on a trinket should contain one theme, while an instructor-led session or web-based presentation can contain numerous themes. (Dissemination techniques will be covered in greater depth in Section 5.) Regardless of the approach utilized, the amount of information should not overwhelm the audience. Brief mention of requirements (policies), the problems that the requirements were designed to remedy, and what the audience should do is all that needs to be covered in a typical awareness presentation or on media.

However, a more complex awareness presentation that incorporates basics and literacy material (see Chapter 3 of NIST Special Publication 800-16) should go into more depth on a particular subject. Since basics and literacy is the bridge between awareness and training, this additional level of detail and complexity is appropriate.

4.2 Developing Training Material

The question to be answered when beginning to develop material for a specific training course is, “What skill or skills do we want the audience to learn?” The awareness and training plan should identify an audience, or several audiences, which should receive training that is tailor-fit to address their IT security responsibilities. NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role-and Performance-Based Model, contains a methodology for building training courses for a number of different audiences. The methodology in the NIST publication will be discussed in this section. Other sources of training courses and material will also be identified and discussed.
4.2.1 A Model for Building Training Courses: NIST Special Pub. 800-16

The methodology in NIST Special Publication 800-16 provides a useful tool with which to develop IT security training courses. This section provides background information on the purpose of the publication and describes how to use the methodology to develop training courses.

Purpose and Methodology: Special Publication 800-16 represents the IT security training needs in the current distributed computing environment, as opposed to the still mainframe-oriented environment of the mid- and late-1980s. The document does this by calling out 26 roles that have some degree of responsibility for IT security. Special Publication 800-16 provides flexibility in its methodology for extension of roles and other parameters to accommodate future technologies and organization roles. The methodology also allows for training courses to be developed at the beginning, intermediate, and advanced levels of training. Sample learning objectives are provided for each level, to guide the course developer. Agencies should consider using the publication to map needed training to new positions that have significant IT security responsibilities.

Using the Special Publication to Develop a Training Course: The NIST Special Publication includes the following resources that a course developer would access, choose from, and use to build a training course:

- The NIST Model (Page 13);
- 26 roles and role-based matrices (Appendix E);
- 46 training matrix cells (Exhibit 4-1, Page 44);
- 12 body of knowledge topics and concepts (Exhibit 4-4, Page 48);
- 3 fundamental training content categories (Pages 43-44); and
- 6 functional specialties (Pages 43-44).

Once an audience has been identified as needing IT security training, Appendix E of the NIST Special Publication can be used to assist in course selection. Agencies can tailor this approach based on specific positions used in their organizations. Appendix E contains 26 matrices, one for each of the 26 roles identified in the publication. Figure 4-1 is a sample matrix for a course for system administrators.
Within each matrix, there are a number of cells that are used to build the course material. There are a total of 46 cells, but only specific cells are used for each course. Some course matrices have as few as two cells, while the course matrix for an IT security officer/manager uses all 46 cells. Most matrices use seven to ten cells.

The matrix is organized by six role categories – or functional specialties – relative to three fundamental training content categories – or training areas (i.e., laws and regulations, security program, and system life cycle security). The six role categories or functional specialties are:

- **Manage** – This category is for individuals who manage IT-based functions in an organization.

- **Acquire** – This category is for those individuals who are involved in the acquisition of IT products and/or services (e.g., serve on a source selection board to evaluate vendor proposals for IT systems). This is especially important for those who serve as a contracting officer’s technical representative (COTR).

- **Design and Develop** – This category is for those individuals who design and develop systems and applications.
- **Operate** – This category is for those individuals who operate (administer) IT systems (e.g., web servers, e-mail servers, file servers, LANs, WANs, mainframes, etc.).

- **Review and Evaluate** – This category is for individuals who review and evaluate (audit) IT functions as part of an organization’s internal controls program, internal review, or an external audit program (e.g., inspector general).

- **Use** – This category is for individuals who access IT resources and/or use IT to do their job.

These are arranged in each matrix along the top, from left to right. There is a placeholder in the seventh column called “Other” that was designed to be used if an additional role category or functional specialty was developed. These six categories allow a training course to be tailor-fit to an audience, taking into account, for example, if a system administrator is managing the function, or is administering (operating) a system or systems. The categories allow the training course to address these roles within a role. Training course material should be organized by role – by an individual’s job function – within the organization.

In Figure 4-1, the sample matrix for a system administrator course, there are ten cells with will be developed to become the course material. Each cell can be seen as a building block for the course material. In this example, most of the cells fall in the “Implement and Operate” specialty or column, since it is assumed that the system administrator will be running (operating) a system or systems. The audience for this course will need to learn something about system management, design, and development, so several of the ten cells are shown in those specialties or columns.

### 4.2.2 Sources of Training Courses and Material

To determine what sources of training material can be useful in building a course(s), it is first necessary to know if the material will be developed in-house or outsourced. If the agency has in-house expertise and can afford to allocate the necessary resources to develop training material and courses, NIST Special Publication 800-16 can be used. In addition, training courses are available that have been developed by other federal agencies that can be edited for far less expense than developing a completely new course. Care should be taken that available material is applicable to the intended audience, and that the material addresses enough of what the prospective attendee needs to know in order to satisfy their IT security responsibilities.

A decision needs to be made regarding in-house development versus outsourcing. Figure 4-2 notes some key issues to consider in making your decision.
• Do we have the in-house resources to do the job? This includes people with the right skills, and enough people to do the work.

• Do we have a person on staff that can serve as the contracting officer’s technical representative (COTR) and effectively monitor contractor activity?

• Does the agency have the necessary resources (e.g., funding and staff with necessary expertise) to maintain the material, if it developed by a contractor?

• Does the course content sensitivity preclude use of a contractor?

• Is there a funding mechanism in place (budget)?

• Does outsourcing allow for critical training delivery schedules to be met?

Figure 4-2: Key Questions – Develop Training Material In-house or Outsource?

If the agency decides to outsource its training course development, there are a number of vendors that offer “off-the-shelf” courses for particular audiences or that can develop courses for specific audiences. Prior to selecting a particular vendor, agencies should have a thorough understanding of what their training needs are and be able to determine, prior to purchasing a course or course development, if a prospective vendor’s material meets their needs.

Maximizing Partnerships: Agencies have more options from which to choose than to simply decide if they will develop training course material with existing resources or outsource. Agencies can establish (or maximize existing) partnerships with other agencies to develop material or coordinate the conduct of training events that meet their IT security training needs. For example, several agencies may combine resources and expertise, and develop a training course for a particular audience. All involved agencies can use the majority of the material developed, as is, if agency-specific material is contained in, and limited to, the first module in the course. Agencies would have to modify or tailor-fit only the module that contains the agency-specific material.

Similarly, an agency might organize a computer security day or an annual or regional conference, and announce that the events are open to other agencies’ personnel. While the material presented might not match exactly what is needed by both agencies, it can be a fairly inexpensive way to meet some of a particular audience’s training needs. If such an arrangement is made, a process must be established to allow each participating agency to track attendance, ensure applicability of the training material, accountability, and other administrative and management issues.
5. **Implementing the Awareness and Training Program**

An IT security awareness and training program can be implemented only after:

- A needs assessment has been conducted;
- A strategy has been developed;
- A training plan (for implementing that strategy) has been completed; and
- Awareness and training material has been developed.

Figure 5-1 shows these key steps leading to the implementation of the awareness and training program.

![Figure 5-1: Key Steps Leading to Program Implementation](image)

5.1 **Communicating the Plan**

The program’s implementation must be fully explained to those in the organization who will be asked to support its implementation and commit the necessary resources. This includes expectations of agency management and staff support, as well as expectations of the results of the program and how its implementation will benefit the organization. Funding issues must also be addressed. For example, agency managers must know if the cost to implement the awareness and training program will be totally funded by the CIO or IT security program budget, or if their budgets will be impacted to cover their share of
the expense of implementing the program. It is essential that everyone involved in the implementation of the program understand their role and responsibility. In addition, schedules and completion requirements must be communicated.

Communication of the plan can be tailored to the three implementation models discussed in Section 3. Typical scenarios follow.

- **Centralized Program Model Communication Scenario**: In this model, the CIO and/or ISSO develop all agency IT security awareness and training policy, develop the strategy, and implement the program. Therefore, all necessary funding for material development and implementation is controlled and provided by the CIO and ISSO. By the time the program is to be implemented, they have conducted the needs assessment, developed the training plan, and developed the awareness and training material. The CIO/ISSO should brief the agency head and senior management on the implementation plan and get approval to communicate it throughout the agency. Once the implementation plan is approved, the CIO/ISSO should communicate the plan to organizational unit management, providing the schedule for awareness and training offerings, and allocating slots in each session, where applicable, for each unit. The organizational unit managers should then communicate the plan to their staff, identify the awareness and training required, schedule attendees, and submit their nominations for each offering to the CIO/ISSO as required.

- **Partially Decentralized Program Model Communication Scenario**: In this model, the CIO and/or the ISSO develop all agency IT security awareness and training policy, and develop the strategy. They also conduct the needs assessment, from which the strategy is derived. Organizational unit managers are then given an awareness and training budget, develop training plans for their own unit, and implement the program. They should provide status reports to the CIO/ISSO as required.

- **Decentralized Program Model Communication Scenario**: In this model, the CIO and/or ISSO disseminate broad policy and expectations regarding the IT security awareness and training program. Execution of the remainder of the program is the responsibility of the organizational units. The organizational unit managers are expected to conduct a needs assessment, formulate a strategy, develop a training plan, develop awareness and training material, and implement the awareness and training program.

Once the plan for implementing the awareness and training program has been explained to (and accepted by) agency management, the implementation can begin. There are a number of ways that awareness material and messages can be presented and disseminated throughout an organization.
5.2 Techniques for Delivering Awareness Material

Many techniques exist to get an IT security awareness message, or a series of messages, disseminated throughout an agency. The technique(s) chosen are dependent upon resources and the complexity of the message(s).

Techniques an agency can consider include, but are not limited to:

- Messages on trinkets (key fobs, post-it notes, notepads, first aid kits, clean-up kits, diskettes with a message, bookmarks, frisbees, clocks, “gotcha” cards, etc.)
- Posters, access lists, and “do & don’t lists”
- Screensavers and warning banners/messages
- Newsletters and desk-to-desk alerts
- Agency-wide e-mail messages
- Videotapes
- Web-based sessions
- Computer-based Sessions
- Teleconferencing sessions
- In-person, Instructor-led Sessions
- Computer security days
- “Brown bag” Seminars
- Rewards program (plaques, mugs, letters of appreciation)

Some techniques that lend themselves to dissemination of a single message are the use of trinkets, posters, access lists, screensavers and warning banners, desk-to-desk alerts, agency-wide e-mail messages, brown bag seminars, and rewards programs.

Techniques that can more easily include a number of messages include “do and don’t lists,” newsletters, videotapes, web-based sessions, computer-based sessions, teleconferencing sessions, in-person instructor-led sessions, and brown bag seminars.

Techniques that can be fairly inexpensive to implement include messages on trinkets, posters, access lists, “do and don’t lists,” screensavers and warning banners, desk-to-desk alerts, etc.
alerts, agency-wide e-mail messages, in-person instructor-led sessions, brown bag seminars, and rewards programs. Appendix C contains sample posters.

Techniques that can require more resources include newsletters, videotapes, web-based sessions, computer-based sessions, and teleconferencing sessions.

5.3 Techniques for Delivering Training Material

Techniques for effectively delivering training material should take advantage of technology that supports the following features:

- **Ease of use** (e.g., easy to access and easy to update/maintain);
- **Scalability** (e.g., can be used for various audience sizes and in various locations);
- **Accountability** (e.g., capture and use statistics on degree of completion); and
- **Broad base of industry support** (e.g., adequate number of potential vendors, better chance of finding follow-on support).

Some of the more popular techniques that agencies can employ include:

- **Interactive video training (IVT)** – IVT is one of several distance learning techniques available for delivering training material. One of the recent developments in this technique is two-way interactive audio and video instruction. The interactive feature makes this – while more expensive than other distance learning techniques – more effective than non-interactive techniques.

- **Web-based training** – This technique is currently the most popular for distributing training material over distances. “Attendees” of a web-based session can study independently and learn at their own pace. Testing and accountability features can be built in to gauge performance. However, this technique does not provide the additional benefit of interaction between instructor and student or among students.

- **Non-web, computer-based training** – This technique was made popular before the advent of the web. It can still be an effective method for distribution of training material, especially if access to web-based material is not feasible. Like web-based training, this technique does not allow for interaction between the instructor and students or among students.

- **On-site, instructor-led training (including peer presentations and mentoring)** – This is one of the oldest, but still one of the most popular techniques for delivering training material to an audience. The biggest advantage of this technique is the interactive nature of the instruction.
6. Post-Implementation

An organization’s IT security awareness and training program can quickly become obsolete if sufficient attention is not paid to trends in technology advancements, infrastructure and organizational changes, as well as shifts in mission and priorities. CIOs and ISSOs need to be cognizant of this and incorporate mechanisms into their strategy to prevent this so that the program continues to be relevant and compliant with overall objectives.

This section discusses techniques that can be used to address this. Continuous improvement should always be the theme for security awareness and training initiatives, as this area is one where “you can never do enough.”

![Diagram: Key Steps Leading to Post-Implementation](image)

**Figure 6-1: Key Steps Leading to Post-Implementation**

6.1 Monitoring Success

Once your program has been implemented, it is essential that processes be put in place to monitor compliance and effectiveness. Support for this normally takes the form of an automated tracking system, which has been designed to capture key information regarding program activity (courses, dates, audience, counts, source, etc.). It should be scoped to capture this data at an agency level so that it can be used to provide enterprise-
wide analysis and reporting regarding awareness, training, and education initiatives. It also makes responding to oversight bodies easier (e.g., auditors, congressional inquiries, OMB, etc). Requirements for the database should incorporate the needs of all intended users. Typical users of such a database would include:

- **CIOs** – Can use the database to support strategic planning, inform the agency head and other senior management officials on the health of the IT security awareness and training program, identify in-house capability and critical needs in security workforce, perform program analysis, identify activity enterprise-wide, assist in security and IT budgeting, identify the need for program improvement, assess compliance, and respond quickly to congressional and oversight requests.

- **ISSOs/Security Program Managers** – Can use the database to support security planning, provide status reports to the CIO and other management and security personnel, justify requests for funding, demonstrate compliance with agency-established goals and objectives, identify vendors and other training sources, respond to security-related inquiries, identify current coverage and make adjustments for critical omissions.

- **Human Resources Departments** – Can use the database to ensure that an effective mechanism exists for capturing all security-related training, identify all IT security-related costs and activity, assist in the establishment of position descriptions, support status reporting, and respond to training inquiries.

- **Agency Training Departments** – Can use the database to assist in developing overall agency training strategy, establish training database requirements tied to security directives, identify possible training sources, support training requests, identify course relevance and popularity, support budgeting activity, and respond to inquiries.

- **Functional Managers** – Can use the database to monitor their employee’s training progress and adjust employee training plans as needed, get status reports and respond to inquiries regarding security training in their components, and identify training sources and costs to assist with budget requests.

- **Auditors** – Can use information from the database to monitor compliance with security directives and agency policy.

- **Chief Financial Officers (CFOs)** – Can use information from the database to respond to budget inquiries, assist in financial planning, and provide reports to the agency head and senior managers regarding security training funding activities.

Security Program Managers play a key role in defining the requirements necessary to support the agency security policy and directives.
Tracking compliance involves an assessment of how the status indicated by the available database information maps to standards established by the agency in this area. Reports can be generated and used to identify gaps or problems. Corrective action and necessary follow-up can then be taken. This may involve formal reminders to management, creating additional training, awareness or education offerings, establishment of a corrective plan with scheduled completion dates, etc.

6.2 Evaluation and Feedback

Formal evaluation and feedback mechanisms are critical components for any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented. Figure 6-2 shows various evaluation and feedback mechanisms that can be used to update the training plan.

![Figure 6-2: Evaluation and Feedback Techniques](image)

A feedback strategy needs to incorporate elements that will address quality, scope, deployment method (e.g., web-based, onsite, offsite, etc.), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

There are many methods applied to solicit feedback. The most common include:

- **Evaluation Forms/Questionnaires** – There are a variety of formats one can use and the best designs eliminate the need for a lot of writing on the part of the person filling them out. The key here is to design these to be as “user friendly” as possible. If possible, work with the experts in your agency who are familiar with the best
techniques for designing these evaluation instruments or seek the assistance of outside experts.

- **Focus Groups** – This involves bringing subjects of the training together in open forums to discuss their perspective on IT security training program effectiveness and solicit ideas for improvement.

- **Selective Interviews** – This approach first identifies training target groups based on impact, priority, or other established criteria and identifies specific areas for feedback. This normally is conducted using one-on-one interviews or in small homogeneous groupings (usually ten or less). This approach is more personalized and private than the focus group approach and may encourage participants to be more forthcoming in their critique of the program.

- **Independent Observation/Analysis** – You may choose to incorporate a review of your IT security awareness and training program as a task to an outside contractor or other third party as part of an agency-initiated audit. This is something the agency would do in addition to the normal oversight activity (OIG, GAO) based on its own interests in getting an unbiased opinion regarding program effectiveness.

- **Formal Status Reports** – A good way to keep focus on security awareness and training requirements agency-wide is to implement a requirement for regular status reporting by functional managers.

- **Security Program Benchmarking (External View)** – Many organizations incorporate “Security Program” benchmarking as part of their strategy for continuous improvement and striving for excellence. *This type of benchmarking is focused on the question: How do I rate among my peers?* The externally focused form of security benchmarking compares an organization’s performance against a number of other organizations and provides a report back to the agency on where they fall based on observed baselines across all organizations with data currently available. A section of this type of benchmarking should include a segment on security awareness and training. This type of benchmarking is normally done by experts in benchmarking techniques who have extensive information (data) across a broad range of organizations over a fairly long duration (five years or more).

### 6.3 Managing Change

It will be necessary to ensure that the program, as structured, continues to be updated as new technology and associated security issues emerge. Training needs will shift as new skills and capabilities become necessary to respond to

Managing change is the component of the program designed to ensure that training/awareness/education deployments do not become stagnant and therefore irrelevant to real emerging issues faced by the organization. It is also designed to address changes in security policy and procedures reflected in the culture of the agency.
new architectural and technology changes. A change in the organizational mission and/or objectives can also influence ideas regarding how best to design training venues and content. Emerging issues in areas such as Homeland and cyber security will also impact the nature and extent of security awareness activity necessary to keep employees informed/educated on the latest exploits and countermeasures. In addition, as security directives change or are updated, awareness and training material should reflect these changes where appropriate.

6.4 Ongoing Improvement (“Raising the Bar”)

This stage of the program is focused on creating a level of security awareness and excellence that achieves a security presence in the organization that can truly be described as pervasive. In other words, the processes that deliver awareness, training, and education to the workforce are totally integrated into the overall business strategy. A defined set of metrics for this area has been established and automated systems are in place to support capturing of quantitative data and delivery of management information to accountable parties on a regular, predefined cycle.

Monitoring, follow-up, and corrective procedures are well-defined and seamless. Finally, in this stage, agencies have incorporated into their awareness and training program formal mechanisms for ongoing research in areas of technology advancement, good practices and benchmarking opportunities. Strategically, the view becomes more external in terms of research focused on moving the program to another level.

Figure 6-3: Raising the Bar
6.5 Program Success Indicators

CIOs and Security Program Managers need to be primary advocates for continuous improvement and support of an agency’s security awareness, training, and education program. It is so critical that everyone be capable and able to carry out their assigned security roles in the organization. Although “passé,” the phrase: “You are only as strong as your weakest link.” is true. Securing an organization’s information and infrastructure is a team effort. Listed below are some key indicators to gauge the support for, and acceptance of, your program.

- Sufficient funding to implement the agreed-upon strategy.
- Appropriate organizational placement to enable those with key responsibilities (CIO, ISSO) to effectively implement the strategy.
- Support for broad distribution (web, email, TV) and posting of security awareness items.
- Executive messages to staff regarding security (staff meetings, broadcasts to all employees by agency head, etc.) showing high-level support for the program.
- Level of attendance at mandatory security forums/briefings.
- Recognition of security contributions (contests focused on awareness such as poster contests and awards focused on security achievements).
- Motivation demonstrated by those playing key roles in managing/coordinating the security program.
Appendix A
Sample Needs Assessment Interview and Questionnaire

Current Assignment (Agency/Office):

Parent Organization (Department/Agency):

Rank or Grade Date of Current Assignment (mm/yy)

JobTitle:

This questionnaire is designed to identify the knowledge, skills and experience you use to administer your organization’s information systems and networks. It asks about functions you perform, how you learned to do them, and the kinds of training you think would be of the greatest benefit to you on the job. The information you provide will be used to design security training to meet the needs of (agency name) system administrators. The questionnaire should take you approximately 30 minutes to complete.

Part 1. Background:

1. Do you currently perform duties as a system administrator? Yes No
   1a. If yes, do you do the job on a full time basis? Yes No
   1b. If less than full time, what percent of time do you spend doing system administration duties? ______%

2. How long have you worked as a system administrator? _____Years _____Months

3. Do you have system administrators working for you? Yes No

4. Do you work for a system administrator? Yes No

5. Did you have formal training in system administration? Yes No
   (If Yes, please specify below)

<table>
<thead>
<tr>
<th>(School or Vendor)</th>
<th>Course Title/Name</th>
<th>(Duration- Days)</th>
<th>(Year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(School or Vendor)</td>
<td>Course Title/Name</td>
<td>(Duration- Days)</td>
<td>(Year)</td>
</tr>
</tbody>
</table>

6. Did you have formal training in system security? (If Yes, please specify below) Yes No

<table>
<thead>
<tr>
<th>(School or Vendor)</th>
<th>Course Title/Name</th>
<th>(Duration- Days)</th>
<th>(Year)</th>
</tr>
</thead>
</table>

7. Please indicate the number of years of formal education you have completed. (e.g., HS = 12 years, BA/BS = 16 years):_____

8. How many seminars or conferences relating to system administration or information systems security have you attended in the last year?______

9. Do you regularly read computer/networking/software journals or magazines? (If yes, please specify below.) Yes No
Part 2. Task Performance and Training:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage System Hardware:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan hardware installation</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Acquire hardware</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Coordinate network</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>installation</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Schedule preventive</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>maintenance</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Coordinate hardware</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>repair</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Install hardware</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Boot system</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Maintain inventory of</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>system hardware</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Order consumable</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>supplies</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Run diagnostics</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Relocate hardware</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Manage System Software:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimize operating</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td>system parameters</td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
<tr>
<td>Plan system changes</td>
<td>[0 L M W D]</td>
<td>Classroom</td>
<td>OJT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Self Study</td>
<td>Other</td>
</tr>
</tbody>
</table>
### Sample Needs Assessment Interview and Questionnaire

**For each task in column A, circle the letter in column B that indicates how often you perform the task:**

- 0 – never
- L – less than once a month
- M – monthly
- W – weekly
- D – daily

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Indicate (✓) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set system defaults</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Generate new operating system kernel</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Maintain system startup/shut down procedures</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Maintain command files</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Test update validity</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Install system software</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Shut down system</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Reboot system</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Maintain software inventory</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Install system changes</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Install vendor specific hardware</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Install system updates or patches</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Maintain documentation</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
<tr>
<td>Plan data storage layout</td>
<td>0 L M W D</td>
<td>Classroom ___ OJT ____ Self Study ___ Other</td>
</tr>
</tbody>
</table>
Appendix A
Sample Needs Assessment Interview and Questionnaire

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Indicate (✓) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>For each task in column A, circle the letter in column B that indicates how often you perform the task: 0 – never  L – less than once a month  M – monthly  W – weekly  D – daily</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan back-up procedures</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Implement back-up procedures</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Monitor data storage use</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Maintain file system integrity</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Audit file system security</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Delete unnecessary files</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Manage log files</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Maintain data storage layout</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Format storage media</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Partition disks</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Create a file system</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Load data</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Restore data from a back-up</td>
<td>0 L M W D</td>
<td>Classroom  Self Study  Other</td>
</tr>
<tr>
<td>Manage Application Software</td>
<td>Evaluate effect of software packages</td>
<td>0 L M W D</td>
</tr>
</tbody>
</table>
For each task in column A, circle the letter in column B that indicates how often you perform the task:
0 – never  L – less than once a month  M – monthly  W – weekly  D – daily

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Put a check indicating the primary way you received your training to do this task. If &quot;Other&quot; please specify (e.g., workshops, trial and error, etc.).</th>
<th>Indicate (✔) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimize application parameters</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Plan application changes</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Ensure compatibility among applications</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Allocate system resources to applications</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Validate integrity of applications before installation</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Test validity of software installation</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Install application software</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Maintain inventory</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Maintain application documentation</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Install application updates</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Plan network connectivity</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Request interhost connectivity</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Acquire Internet address</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Build network cables</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
<tr>
<td>Configure TTY lines</td>
<td>0 L M W D</td>
<td>__Classroom ____ OJT ____ Self Study ____ Other</td>
<td></td>
</tr>
</tbody>
</table>
### Sample Needs Assessment Interview and Questionnaire

**Appendix A**

For each task in column A, circle the letter in column B that indicates how often you perform the task:
- **0** – never
- **L** – less than once a month
- **M** – monthly
- **W** – weekly
- **D** – daily

#### Task List

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure peripheral lines</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Configure file servers and clients</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Configure firewalls</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Monitor network activity</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Manage network services</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Manage network bridges and routers</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Manage print servers</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Manage terminal servers</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Manage network topology</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Assign addresses to nodes</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Install network software</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Set access permissions</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Start network software</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Test communication connectivity</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
<tr>
<td>Stop network software</td>
<td>0 L M W D</td>
<td>_</td>
<td>_</td>
<td>_</td>
</tr>
</tbody>
</table>

Put a check indicating the primary way you received your training to do this task. If "Other" please specify (e.g., workshops, trial and error, etc.).

Indicate (✓) if you think you could use more training on the task.
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>Put a check indicating the primary way you received your training to do this task. If &quot;Other&quot; please specify (e.g., workshops, trial and error, etc.).</th>
<th>Indicate (✓) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-establish host connectivity</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Help establish audit guidelines</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Help establish user security guidelines</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist writing system security plans</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist in host network accreditation</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Ensure output labeling procedures</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Ensure data labeling procedures</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist testing security mechanisms</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist in analysis of audit trails</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist in incident handling</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Enforce security procedures</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist in maintaining physical security for the system</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Assist in maintaining device access controls</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Report security incidents</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Manage Accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Sample Needs Assessment Interview and Questionnaire

For each task in column A, circle the letter in column B that indicates how often you perform the task:
0 – never  
L – less than once a month  
M – monthly  
W – weekly  
D – daily

<table>
<thead>
<tr>
<th>Task</th>
<th>A</th>
<th>B</th>
<th>Put a check indicating the primary way you received your training to do this task. If &quot;Other&quot; please specify (e.g., workshops, trial and error, etc.).</th>
<th>Indicate (✔) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan account management strategy</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish user login environments</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assist ISSO in managing mandatory access controls</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage account privileges</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit account activity</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage resources used by account</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add new accounts</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assist in setting the account’s access control list</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explain basic operating procedures</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assist in modifying passwords</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete accounts</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Troubleshoot Problems</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recreate problem scenarios</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interpret error messages</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test components</td>
<td>0 L M W D</td>
<td>__Classroom ___ OJT __ Self Study ___ Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Draft: July, 2002**
### Appendix A
#### Sample Needs Assessment Interview and Questionnaire

For each task in column A, circle the letter in column B that indicates how often you perform the task:

- **0** – never
- **L** – less than once a month
- **M** – monthly
- **W** – weekly
- **D** – daily

<table>
<thead>
<tr>
<th>Task</th>
<th>A</th>
<th>B</th>
<th>Indicate (✓) if you think you could use more training on the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isolate problems</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Maintain log of problems and solutions</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Recover from system crashes</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Respond to user identified problems</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Gather troubleshooting information</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Use diagnostic tools</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
<tr>
<td>Initiate corrective action</td>
<td>0 L M W D</td>
<td>___Classroom ___OJT ___Self Study ___Other</td>
<td></td>
</tr>
</tbody>
</table>

Put a check indicating the primary way you received your training to do this task. If "Other" please specify (e.g., workshops, trial and error, etc.).
**Part 2. Task Performance and Training (cont.):**

Use the table below to indicate any other system administration functions you perform that are not covered above. For each, indicate how often you perform the task, the primary way you were trained to do the job, and whether you think more training would help you do the task.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
<tr>
<td>0 L M W D</td>
<td>Classroom</td>
</tr>
</tbody>
</table>

Put a check indicating the primary way you received your training to do this task. If "Other" please specify (e.g., workshops, trial and error, etc.).

Indicate (✔) if you think you could use more training on the task.
Part 3. Job Task Discussion:

1. Are you required to: (✔)
   ___Install firewalls?
   ___Operate firewalls?
   ___Maintain firewalls?

2. If you checked any responses in question 1 please specify:
   The number of firewalls ______
   The type of hardware ________________________________________________
   What software you work with_________________________________________

3. Are you required to install: (✔)
   ___Network cables
   ___PCs/workstations
   ___Routers/bridges
   ___Security-related hardware
   ___Security-related software
   ___Other software

4. Does your job require you to know how to program or write shell scripts?  Yes  No
   In which language(s)?________________________________________________

5. What kinds of functions/programs have you written in the last year? (✔)
   ___Cron jobs
   ___Login functions
   ___Back-ups
   ___Restore
   ___Accounting functions
   ___Other (please specify)_____________________________________________

6. What kinds of scripts or programs do you maintain? (✔)
   ___Cron jobs
   ___Login functions
   ___Back-ups
   ___Restore
   ___Accounting functions
   ___Other (please specify)_____________________________________________

7. Do you share system duties with any of the following (Indicate the number of each)
   ___Network administrator(s) __________
   ___Database administrator(s) _________
   ___Other SA(s) __________
   ___ISSO/ISSM(s) _________

8. Do you administer more than one network?  Yes  No
9. What operating systems and versions are used in your system? (e.g., Solaris 2.5.1, Windows NT 4.0 Sp6a, Redhat Linux 6.0)

_________________________________________________________________

10. Are you responsible for system security? Yes No
    If YES, what instruction or policy defines that duty?_________________________

11. What specific programs do you use for each of the following (for each, please indicate if its use is optional (O), or required (R) by your command or organization):

<table>
<thead>
<tr>
<th>Program</th>
<th>Required (R)</th>
<th>Optional (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network mapping</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit functions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password checking or enhancement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12. Are you a certified system administrator? Yes No
    If Yes, what specific training courses (classroom, CDs, CBTs, etc) and/or test(s) did you take to be certified?_____________________________________________________________
    ___________________________________________________________________
    ___________________________________________________________________
    ___________________________________________________________________

13. What do you feel are your top five information system security training needs? (for each, indicate whether your need is for basic, intermediate or advanced training)
    A.___________________________________________________________________
    B.___________________________________________________________________
    C.___________________________________________________________________
    D.___________________________________________________________________
    E.___________________________________________________________________

14. Additional comments:
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________
_____________________________________________________________________  
_____________________________________________________________________  

Thank you for participating in this survey.
*AGENCY NAME HERE*

COMPUTER SECURITY

AWARENESS & TRAINING

PROGRAM PLAN

VERSION 1.0
# TABLE OF CONTENTS

- EXECUTIVE SUMMARY ................................................................. 4
- BACKGROUND ............................................................................... 4
- INTRODUCTION ............................................................................ 5
- MISSION .......................................................................................... 5
- PROPOSED (AGENCY NAME) POLICY ........................................... 5
- RESPONSIBILITIES ......................................................................... 6
- AWARENESS .................................................................................. 6
  - GOALS .......................................................................................... 6
  - LEARNING OBJECTIVES ........................................................... 6
  - LEARNING TOPICS .................................................................... 7
  - LEARNING METHODS/ACTIVITIES ........................................... 7
  - APPROACH ............................................................................... 9
  - DOCUMENTATION/EVIDENCE OF LEARNING.......................... 9
  - EVALUATION ............................................................................ 9
- TRAINING ........................................................................................ 10
  - GOALS ...................................................................................... 10
  - LEARNING OBJECTIVES .......................................................... 10
  - LEARNING TOPICS .................................................................. 10
  - LEARNING METHODS/ACTIVITIES ....................................... 12
  - APPROACH ............................................................................ 13
  - DOCUMENTATION/EVIDENCE OF LEARNING....................... 13
  - EVALUATION .......................................................................... 13
- EDUCATION .................................................................................... 13
  - GOALS ...................................................................................... 13
Appendix B
Sample Awareness and Training Plan

LEARNING OBJECTIVES ...................................................... 14
LEARNING TOPICS ............................................................ 14
LEARNING METHODS/ACTIVITIES .............................. 14
APPROACH ....................................................................... 14
DOCUMENTATION/EVIDENCE OF LEARNING .................. 14

**PROFESSIONAL CERTIFICATION** .............................................. 14

GOALS ............................................................................. 14
LEARNING OBJECTIVES ...................................................... 14
LEARNING METHODS/ACTIVITIES ..................................... 14
APPROACH ....................................................................... 15
DOCUMENTATION/EVIDENCE OF LEARNING .................. 15
EVALUATION ................................................................... 15

Draft: July, 2002

B-3
COMPUTER SECURITY AWARENESS & TRAINING PROGRAM PLAN

EXECUTIVE SUMMARY

It is the intent of the Computer Security Awareness & Training Program to make users aware of (agency name) computer and information security responsibilities and to provide each user with the knowledge needed to implement (agency name) computer security policies and recommended computer security practices. To be truly effective, everyone must do his/her part to secure (agency name) information technology environment. As the use of information technology and electronic services continue to grow, risks impacting the integrity, confidentiality and accessibility of data also increases.

Since information is our major product, unprotected information systems can have serious consequences, including:

- The inability of (agency name) to perform its mission
- Public embarrassment and loss of credibility to (agency name)
- The waste, loss, or misappropriate use of (agency name) funds

To do our jobs, we must have information available when we need it; it must be accurate, and we must know the steps needed to safeguard its confidentiality when necessary. As users of (agency name) automated information systems, we must be able to recognize potential computer security situations and the appropriate steps to avert them. For (agency name) programs to achieve their objectives, each of us needs to assume responsibility for computer security.

BACKGROUND

The 1987 Computer Security Act, Public Law 100-235 states its purpose “to require mandatory periodic training for all persons involved in the management, use, or operation of Federal computer systems that contain sensitive information.” Section 5.a of the same Act details that “each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice 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.” In support of this mandate, the (agency’s department name) (department regulation section) titled Security Awareness and Training specifies policy that each (department name) sub-agency shall:

- Establish an information technology (IT) awareness and training program;
- Provide an awareness briefing as part of employee orientation within 60 days;
- Provide awareness refresher briefings;
- Provide specialized training to those who design, implement or maintain systems; and
- Provide specialized training to those who are assigned responsibilities for IT security...
The Computer Security Act further states that training will be provided in accordance with guidelines co-developed by the National Institute of Standards and Technology (NIST) and the Office of Personnel Management. NIST Special Publication 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model”, provides guidance and distinguishes between information technology security awareness and training.

**INTRODUCTION**

Based on NIST SP 800-16, Departmental guidance, and Federal mandates, this document outlines the (agency name) computer security awareness & training program for those systems and information which are considered sensitive and unclassified. The document discusses goals, learning objectives, learning topics, learning methods/activities, documentation/evidence of learning, and evaluation for each of the two programmatic categories: awareness and training. Federal computer security guidance does not require inclusion of education in this plan. The answer to when training becomes education is currently being debated in professional interagency groups such as the Federal Information Systems Security Educators Association (FISSEA). Hence, professional certifications, which can be either training or education are included within this plan separately.

It is important to note that this document is a “living document” which will be regularly reviewed and updated. Updates will address changes in (agency name) policies, IT architecture and computing environment, as well as changes in attitudes and culture of (agency name) staff, contractors, students, guest researchers, collaborators, and partners.

**MISSION**

The (agency name) IT Security Program will establish and maintain a computer security awareness and training program in accordance with Federal regulations and Departmental policy. Initial, overall goals include increasing awareness and providing the training and tools necessary for the proper management and use of (agency name) IT resources.

**PROPOSED (AGENCY NAME) POLICY**

All who manage, use, or operate (agency name) internal electronic information and resources will successfully complete a Basics and Literacy awareness course as a refresher or within the first 60 days of initial access. Course may count toward completion of training requirements.

Supervisors, managers, and computer security officers will successfully complete computer security training to produce relevant and needed security skills and competency to support their leadership role. Course may count toward required supervisory training as well as training requirements. System administrators, web masters, information coordinators, and other functional roles as deemed necessary by the (agency name) CSO will successfully complete computer security training to produce relevant and needed security skills and competency to support protection of (agency name) information and resources.

*Draft: July, 2002*
Responsibilities

1. (agency name) Computer Security Officer
   Establish and maintain computer security awareness and training program, recommending methodologies and materials, suggesting and implementing approaches based on (agency name) computer security environment and policies.

2. Organizational Unit Computer Security Officers (OU CSOs)
   Provide feedback and assist with design and implementation of awareness and training program and its effectiveness. Acquire the necessary training to adequately perform the duties of OU CSO.

3. OU Directors, Division Chiefs, Group Leaders, and Project Managers
   Ensure that (agency name) staff, contractors, guest researchers, students have the necessary awareness and computer security training.

4. System administrators, web masters, information coordinators, and other functional roles
   Acquire specialized training to develop and maintain (agency name) computers in compliance with (agency name) and Departmental policies and Federal regulations.

Awareness

The purpose of awareness is to focus attention on security, creating sensitivity to the threats and vulnerabilities of computer systems and recognition of the need to protect data, information, and systems. Because attention to security tends to dissipate over time, regular and focused awareness efforts have the potential to reinforce recommended security practices.

Goals

- To focus attention on computer security.
- To create a sensitivity to threats and vulnerabilities.
- To reinforce recommended security practices.

Learning Objectives

An effective awareness program will reduce the number of accidental security incidents because people will be more conscious of general security issues. It will also reduce the damage caused by incidents because people will have more knowledge of how to avoid general security problems and
will know how to obtain information and tools to adequately respond to incidents. An effective awareness program reinforces desired behaviors and gradually changes undesired behaviors through persistent, long-term efforts. Repetition is important and so is variety of the method by which the message is delivered.

**Learning Topics**

Anyone involved in the management, use, or operation of (agency name) electronic information and systems should be involved in awareness efforts. Learning methods, or activities, should concentrate on a particular topic, and those topics should be rotated to prevent a particular topic from becoming stale and unnoticed. Topics include, but are not limited to:

- (department name) and (agency name) policies,
- (agency name) adverse actions,
- social engineering threats,
- password management
- physical security
- anti-virus software
- incident handling and reporting
- risk management
- copyright compliance
- information assurance
- contingency planning (backup and recovery)
- media disposal
- labeling information and media

**Learning Methods/Activities**

Awareness at (agency name) is currently accomplished in the form of broadcast email alerts/advisories, web pages, warning banners, logon banners, and meetings relative to security topics. While these vehicles continue to heighten awareness, specific non-technical activities are necessary to discover, direct, and promote an overall level of awareness appropriate for everyone. Activities include the following:

Broadcast emails capture the widest audience when sending alerts and advisories. These emails are typically sent by the (agency name) Computer Security Officer or designate to specific groups (unix-admin, nt-admin, public-net, allstaff), and are archived on the (agency name) Computer Security web site. Because of (agency name) diverse computing environment, this continues to be the best means of sending alerts and advisories. Alternative options, such as broadcast phone messages, may be evaluated in the future.

Currently, (agency name) *Recommended Computer Security Procedures* include the presence of a warning banner when logging into a multi-user system. This recommended practice supports Federal mandates, and should be continued.

The (agency name) Computer Security Web Site has become a primary means of making policies, procedures, and other computer security information available to (agency name) staff. The
redesigned site is currently maintained, and additions are made at least weekly. Most, if not all government agencies house their policies on internal web sites.

Posters around the agency could reinforce specific computer security topics. Placing eye-catching posters with simple messages around the agency will help reinforce recommended security practices, and remind users of specific computer security topics. Given the number of topics, posters could be created one per topic and duplicated to accommodate the number of designated sites. The poster topic should be changed on a monthly, bi-monthly, or quarterly cycle. Numerous agencies use posters as a means of reinforcing computer security practices and topics.

(Agency name) created a series of internal informational flyers on various computer security topics. This has proven to be an effective practice at (agency name). At a minimum, (agency name) should reformat its IT Resources Access and Use Policy and distribute it in the form of a smaller flyer, and include reference to the (agency name) Computer Security web site. Other topics could include:

- Passwords and You
- What should you do if you have a virus?
- Why do we need computer security?
- Network Security Guidelines
- Incident Response
- Workstation Security Guidelines
- Desktop Security Guidelines
- Junk E-mail
- Malicious Software
- How to Install, Update, and Run Desktop Anti-Virus Software
- Disposition of Your System and Media

(A number of departments and agencies) publish computer security newsletters. While (agency name) already has many publications of a general nature, a newsletter published quarterly dedicated solely to computer security should heighten awareness to specific topics, issues, and events. The newsletter would be distributed to all staff electronically, and archived on the (agency name) Computer Security web site. Of the agencies previously mentioned, four continue to receive positive feedback on the quarterly newsletter, while one dropped this activity based on negative feedback.

An annual (agency name) Computer Security Day could highlight topics of a non-technical, general nature for all (agency name) staff. In addition to speakers and presentations, the (agency name) Computer Security Day could include exhibition of security products from vendors, contests, and security-related prizes. The same activities could be coordinated with (department name), (other agency name), and (third agency name) for the (other agency site) facilities.

A Security Mascot would add humor to computer security posters and flyers. The mascot could be proposed by a (agency name) staff member and designed by the (agency name) Visual Arts group. The advantage of having a mascot is that users would associate security to the mascot, which could add an element of humor or fun.
to messages, brochures, posters, and newsletters. A contest for suggestions could be an activity of a (agency name) Computer Security Day.

Contests (such as suggestions for a security mascot or catchy phrases for new slogans) could add creativity to the (agency name) Computer Security Day.

Security trinkets and prizes such as mouse pads, key chains, badge holders, biometric devices, laptop locks, t-shirts, and anti-virus CDs could be given away. Each could contain a “slogan” to reinforce security topics. Security slogans could include:

- “You are the key to security … respect copyrights.”
- “Information protection is everyone’s business.”
- “Computer viruses are always in season.”
- “Copyright compliance is the law.”
- “Information is an asset. Let’s protect it.”
- “Nothing personal … your email is government property.”
- “Sec_rity is not complete without U!”

Awards could be used to identify and reward individuals and groups for creative and effective incident handling and volunteer participation in security related efforts.

A library of computer security videos and CD ROMs continue to be made available for employee loan. This library is comprised of videos and CD ROMs received free from other agencies. Periodic evaluations of the contents of the library and providing detailed documentation would promote better use of this resource.

**APPROACH**

As budget and time permits all of the above mentioned learning methods/activities should be explored and implemented towards satisfying Awareness goals. See Appendix for schedule and budgeting information.

**DOCUMENTATION/EVIDENCE OF LEARNING**

While success of awareness is hard to measure, the program should allow for verbal or electronic feedback from employees. Feedback from employees, management, and users would be solicited through formal and informal means. In addition, the outcome of (department name) Office of Inspector General audits and staff feedback would also assess the effectiveness of awareness activities.

**EVALUATION**

Comments and feedback, verbal or otherwise, would be addressed and could result in redirecting the efforts of this program. Awareness topics and activities should be constantly reviewed and changed, thus promoting new, fresh ideas.
TRAINING

The purpose of training is to produce relevant and needed security skills and competency to enable employees, guest researchers, students, collaborators, contractors, and partners to perform their jobs more effectively. Training is the process through which we inform users of (agency name) security policies and practices, what is expected of them, and how they are to handle (agency name) information, data, and systems. Training is arguably one of the most important aspects of computer and information security, and builds on awareness.

GOALS

- To make computer security everyone’s responsibility.
- To provide general computer security training for all who manage, use, or operate (agency name) information and resources.
- To provide specialized computer security training to produce relevant and needed security skills and competency based on functional role or responsibility.
- To provide information on technical conferences, seminars, and symposia related to computer security which result in professional security certification(s)

LEARNING OBJECTIVES

Training will enable individuals to perform more effectively by building the knowledge and skills to facilitate job performance based on a functional role (versus position), such as: manage, acquire, design and develop, implement and operate, review and evaluate, use, and other roles. These role categories map to the following learning topics.

LEARNING TOPICS

Three general areas should be addressed by the training at beginner, intermediate, and advanced levels:

1. Laws and Regulations: Training to provide information on federal government-wide and organization-specific published documents (laws, regulations, policies, guidelines, standards, and codes of conduct) for the management and protection of information technology resources.

2. Security Program: Overview of establishment, implementation, and maintenance of security controls to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored, or disseminated in its general support or major application systems.
   a. Planning: The design and establishment of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision-making
activities; these encompass such elements as organization-specific scope and content, including: policy, guidelines, needs identification, roles, responsibilities, and resource allocation.

b. Management: The implementation and use of organizational structures and processes for IT security program goal-setting, prioritizing, and related decision making activities; these encompass such elements as organization-specific policies, guidelines, requirements, roles, responsibilities, and resource allocation.

3. System Life Cycle Security: The system life cycle is a model for building and operating an IT system from its initial inception to its termination and disposal of assets. The model typically includes six phases, as defined below. Life cycle security is the ensemble of processes and procedures, which ensures data confidentiality, as needed, as well as data and system integrity, and availability.

a. Initiation: The series of steps followed to ensure that security requirements are considered and resolved as new information systems and technologies are planned.

b. Development: The series of steps followed to ensure that security requirements are considered, resolved, and incorporated as information systems and technologies are developed or changed.

c. Test and Evaluation: The series of steps followed to ensure that the design and construction of a new or modified information system or technology has successfully incorporated appropriate security safeguards.

d. Implementation: The development and installation of the system into the operational environment in a manner that does not compromise the integrity and effectiveness of the successfully tested security safeguards.

e. Operations: Includes the ongoing day-to-day use (production) and maintenance or enhancement of the system without compromising the integrity and effectiveness of the installed safeguards.

f. Termination: The series of steps taken to retire a system when it is no longer needed and to securely and properly archive or dispose of its assets.

A fourth learning topic is necessary to serve as a “catch-all” for agency specific topics, and may not require levels beyond the beginner:

4. Other

a. Basics and Literacy: As the bridge between awareness and training, this topic would include introduction of the concepts behind computer security practices and the importance of the need to protect information from known threats. Concepts to include: (agency name) computer security policies, adverse actions, social
Appendix B
Sample Awareness and Training Plan

engineering, password selection and protection, physical security, anti-virus software, incident reporting, threats, risks, copyright compliance, and information assurance.

b. Basics and Literacy for Collaborators, Business Partners, and Contractors: As the bridge between awareness and training, topic would include introduction of the concepts behind computer security practices and the importance of the need to protect information from known threats. Concepts to include: (agency name) computer security policies, adverse actions, social engineering, password selection and protection, physical security, anti-virus software, incident reporting, threats, risks, copyright compliance, and information assurance.

c. Remote and Wireless Access: Introduction of how to securely access (agency name) resources via offsite locations, as well as using wireless technologies. Topics include anti-viral protection, password selection and protection, social engineering, etc.

d. Introduction to Encryption: Introduction to the concept of encryption. Particularly helpful to those who want to purchase and use software for encryption and decryption of information.

e. Anti-virus Protection: Specialized training to provide information on the various types of anti-virus protection, what the (agency name) standard is, how it functions, and how to update signature files. Also, specialized training on how to deal with particular cases of viruses.

f. Incident Handling and Response, et. al.

Learning Methods/Activities

Instructor led or face-to-face communications is the most personal. This type of training offers an ease of interaction between the presenter and the audience. This is, however, the most expensive and labor intensive form of communication.

Computer-based training (CBT) allows for widespread communications. This is a great concept for off-site contractors and collaborators who do not have access to (agency name) electronic resources, but have access to (agency name) information. While many agencies are using CBT for their training, most do not have a means to track and report completion.

Web-based training (WBT) is a way of delivering computer-based training to widespread, limitless audiences across campuses. Training is delivered on the web as compared to local server, CD, or local workstation. WBT can interact with other databases such as a human resources database to track and monitor completion. The (department name) is currently looking at WBT vendors for department-wide use for many forms of computer training.
**APPROACH**

This plan recommends focusing initial efforts on making computer security everyone’s responsibility and providing WBT training for (agency name) employees and non-employees (Basics and Literacy course), and tracking completion within a 60-day timeframe. Consequently, at the end of training period, employees and non-employees will have the same level of knowledge with respect to computer security basics and literacy. During the same period, employees and non-employees will be required to submit to their Administrative Officer, a statement certifying that they understand the *(agency name)* Policy on IT Resources Access and Use. This statement will be retained for the duration of their access to *(agency name)* resources. Annual re-briefing will be required to address changes in *(agency name)* policies, technological architecture and computing environment. See Appendix for schedule and budgeting information.

Additionally, it is recommended that a CBT course be developed and deployed for collaborators, business partners, and contract staff who, within the terms of their contract or agreement, use *(agency name)* information or electronic resources. For those who have electronic access to *(agency name)* resources, the same course in WBT format will be made available. As budget and time permits, specialized training in support of current policies should be designed and deployed in WBT and CBT format. Specialized training includes Remote and Wireless Access, Introduction to Encryption, Anti-virus Protection, Incident Handling and Response, et. al.

**DOCUMENTATION/EVIDENCE OF LEARNING**

Progress should be documented and monitored as part of the employee rating process. Examinations could be used to determine how well people understood the presented materials. For collaborators, business partners, and contract staff, understanding of *(agency name)* computer security policies and procedures should be part of the contract award process.

**EVALUATION**

Formal course evaluations and feedback.

**EDUCATION**

Education is a separate learning level limited to *(agency name)* designated IT security specialists. NIST SP 800-16 takes the view that education (as distinguished from training) and associated job experience are essential for IT security specialists to perform their jobs effectively. Education combines a more formal course of study and on-the-job experience into a common body of knowledge, and provides for more exploration consisting of a broad range of security topics. It is intended for designated IT security specialists *in addition* to role-based training as noted above. Formal course study includes college or university course work or curriculum.

**GOALS**

- To provide information on computer and information security curricula
**LEARNING OBJECTIVES**

Education will enable individuals to perform more effectively by building the knowledge and skills, which encompass a broad range of information and computer security knowledge.

**LEARNING TOPICS**

The entire realm of computer and information security, encompassing a broad range of topics.

**LEARNING METHODS/ACTIVITIES**

Enrollment in college or university course(s) or curricula directly related to computer or information security.

**APPROACH**

Education opportunities will be identified, documented, and disseminated for those employees whose duties require specialization in computer and information security.

**DOCUMENTATION/EVIDENCE OF LEARNING**

Receipt of Bachelor or Master level degree with a major in information or computer security.

**PROFESSIONAL CERTIFICATION**

Professional certifications offer the means, via testing and evaluation, to establish a baseline of knowledge within the field of computer and information security.

**GOALS**

- To ensure a consistent level of knowledge amongst similar functional roles

**LEARNING OBJECTIVES**

Professional certification for similar functional roles will ensure a consistent level of ability by testing knowledge of security risks and skill in implementing good security practices. And thus creates a baseline of knowledge for various similar roles within the organization. Those roles include supervisors, managers, and computer security officers, as well as system administrators, web masters, and information coordinators.

**LEARNING METHODS/ACTIVITIES**

Using either instructor led or web-based training, Professional Certifications demonstrate a certain measurable level of skill, and are quickly gaining popularity amongst employees, government and industry.
APPRAOCH

The (agency name) Computer Security Awareness and Training Program should provide on-site and/or on-line access to professional certification programs for functional roles such as System Administrators, web masters, information coordinators, computer security officers, managers, and supervisors.

DOCUMENTATION/EVIDENCE OF LEARNING

Receipt of professional certification.

EVALUATION

Feedback from participants would be helpful to the organizations providing the certification and to (agency name) to assist in providing more effective guidance.
APPENDIX C

SAMPLE AWARENESS POSTERS
PINKEY USES IT SECURITY.
HER PC IS BEHIND A FIREWALL.

AND SHE KEEPS THE MOST CURRENT VERSION OF HER ANTI-VIRUS SOFTWARE INSTALLED.
PINKEY AND DINKEY DON'T.

http://www.ihs.gov/cio/itsecurity/posters/index.cfm

ITS Information Technology Security
SPONSORED BY INDIAN HEALTH SERVICE
Pinkey Can Be Counted on to Follow the IT Security Policies and Procedures.

http://www.cert.org/security-improvement/index.html

Information Technology Security
Sponsored by Indian Health Service
PinKEY Doesn’t Open E-Mail From STRANGERS.

She Also Does NOT Send Files Ending In:

.VBS, .SHS, .SCR, .EXE, .BAT, .COM, .PIF, .LNK, .SHB, .VB, .WSH, .WSF, .WSC, .SCT, OR .HTA,

As Attachments to Her Emails.

http://www.ibs.gov/cio/itsecurity/posters/index.cfm

Information Technology Security

Sponsored by Indian Health Service