NIST Special Publication 500-172

Technology

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

NIST

Computer Security Training Guidelines

Mary Anne Todd
Constance Guitian

The National Institute of Standards and Technology[1] was established by an act of Congress on March 3, 1901. The Institute's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Institute conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NIST work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Institute's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the National Computer Systems Laboratory, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Computing and Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

The National Computer Systems Laboratory

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Laboratory consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Institute-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3] Located at Boulder, CO, with some elements at Gaithersburg, MD.

NIST Special Publication 500-172

Computer Security Training Guidelines

Mary Anne Todd
Constance Guitian

National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

November 1989

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Acting Director

NIST

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) has a unique responsibility for computer systems technology within the Federal government. NIST's National Computer Systems Laboratory (NCSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. NCSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. NCSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports NCSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

Library of Congress Catalog Card Number: 89-600771
National Institute of Standards and Technology Special Publication 500-172
Natl. Inst. Stand. Technol. Spec. Publ. 500-172, 38 pages (Nov. 1989)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1989

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

EXECUTIVE SUMMARY

The Computer Security Act of 1987, P.L. 100-235, was enacted to improve the security and privacy of sensitive information in Federal computer systems. As one way of meeting that goal, the law requires that "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."

The National Institute of Standards and Technology (NIST) is responsible for developing standards, providing technical assistance, and conducting research for computers and related systems. These activities provide technical support to government and industry in the effective, safe, and economical use of computers. With the passage of P.L. 100-235, NIST's activities also include the development of standards and guidelines needed to assure the cost-effective security and privacy of information in Federal computer systems.

In fulfilling this responsibility, NIST has developed this document to provide a framework for identifying computer security training requirements for a diversity of audiences who should receive some form of computer security training. It focuses on *learning objectives* based upon the extent to which computer security knowledge is required by an individual as it applies to his or her job function.

These guidelines divide employees involved in the management, operation, and use of computer systems into five audience categories:

- **Executives**
- **Program/Functional Managers**
- **IRM, Security, and Audit Personnel**
- **ADP Management, Operations, and Programming Staff**
- **End Users**

These guidelines identify five training content, or subject matter, areas. The level of training required in each area will vary from general awareness training to specific courses in such areas as contingency planning, depending upon the training objectives established by the agency. The five areas are:

- **Computer Security Basics**
- **Security Planning and Management**
- **Computer Security Policies and Procedures**
- **Contingency Planning**
- **Systems Life Cycle Management**

The actual selection of the computer security training will depend upon the specific security responsibilities involving duties assigned to individual personnel.

This document is intended to be used by agencies as guidance in developing, acquiring, evaluating or selecting training courses in computer security.

TABLE OF CONTENTS

INTRODUCTION

PURPOSE AND SCOPE

The Computer Security Act of 1987 (P.L. 100-235) was passed because "improving the security and privacy of sensitive information in Federal computer systems is in the public interest..." The law assigns to the National Institute of Standards and Technology the responsibility for developing guidelines for the training of employees who process sensitive information. The law further states that "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."

This guideline provides a framework for determining the training needs of employees involved with computer systems. It describes the learning objectives of agency computer security training programs. A focus on learning objectives -- what the employee should know and be able to direct or actually perform -- is a generic way to write the guidelines so that agencies may use the guidance in developing, acquiring, evaluating, and selecting training courses in computer security that fit the agency environment. This approach also allows agencies to state clearly the purpose of the training so that effectiveness can be measured by determining how many of the learning objectives have been met.

The training outlined in these guidelines should be incorporated as much as possible into existing training programs rather than as a separate training program. For example, security awareness training could be included in orientation programs for new employees. All training courses involved with automated information systems equipment and software packages could include modules on computer security responsibilities. As training for managers and supervisors is redesigned, it could include modules on computer security in the area of planning and management, policy and procedures, contingency planning and systems life cycle management.

The guidance contained in this document applies to managers, operators, and users of all agency computer systems, both large and small. The basic principles of computer security apply to office information systems and personal computers as well as medium to large mainframe systems.

USING THE GUIDELINES

The law requires that employees responsible for the management, operation, and use of computer systems receive training in computer security awareness and acceptable computer practices. This guide divides these employees into five audience categories:

- **Executives**
- **Program/Functional Managers**
- **IRM, Security, and Audit Personnel**
- **ADP Management, Operations, and Programming Staff**
- **End Users**

The groupings are based on the fact that employees within a given category generally need to know or be able to perform the same or similar types of tasks. But this does not mean that every employee in the group must be trained to do all the tasks. Agencies will determine specific

training needs to assure that each employee receives the appropriate training.

In addition to the audience categories discussed above, this guide also identifies five training content areas (e.g., computer security basics, security planning and management) and assumes that each audience category requires some level of training in each of the five training areas. For example, (refer to the Training Matrix), Program Managers and End Users (two different audience categories) both need training in security planning and management, a single training area. However, Program Managers usually have direct responsibility for the planning for and management of security in the computer systems that support their program areas, while end users typically need only be aware of security planning and management activities. Thus, the level of training for Program Managers and End Users in the security planning and management area is Implementation and Basic, respectively. There may be situations where employees require knowledge only in some of the training subject areas. In these cases, the agency will design a training program by selecting those topics that provide the employees with the skills at the level appropriate to their current position. Many employees may fall into more than one audience category because they will be End Users and something else (e.g., Program Manager). These employees should receive both types of training.

DOCUMENT OVERVIEW

There are five training content, or subject matter, areas:

- **Computer Security Basics**
- **Security Planning & Management**
- **Computer Security Policy and Procedures**
- **Contingency Planning**
- **Systems Life Cycle Management**

Each of these is explained under "Training Content Areas" section of this document.

There are four training levels:

- **Awareness**
- **Policy**
- **Implementation**
- **Performance**

The level of training required in each area will vary from general awareness training to specific courses in such areas as contingency planning, depending upon the training objectives established by the agency. The learning objectives at the appropriate training level for the audience are listed for each training content area. Different audiences may be expected to reach the same training level but the learning objectives may be different. For example, Program and Functional Managers and ADP Management personnel are both to be trained to the Performance level in Contingency Planning. Functional Managers must be able to identify critical workload, establish priorities, and assure the adequacy of contingency plans relating to the safety and availability of data supporting their function. The managers of ADP facilities must assume primary responsibility for developing emergency response plans, and backup and recovery plans for DP-supported functions which meet the requirements of the Program or Functional Managers. Thus, while each has implementation responsibilities in contingency planning, the learning objectives would be different due to the differences in the way they implement contingency planning in their job

functions.

To use these guidelines, an agency should, for each audience category, design training which meets the learning objectives for that group. As an example, executives should receive ***awareness*** level training in computer security basics, and ***policy*** level training in security planning and managing. The **TRAINING MATRIX** included in this document can assist agencies in making these decisions.

CROSS REFERENCES TO EXISTING PUBLICATIONS

These guidelines provide a listing which cross-references the training content areas to some of the existing publications which course developers and agency training officers may find useful in obtaining information and guidance in each topical area. Among the references are publications developed by the National Institute of Standards and Technology in its role to improve the utilization and management of computers and automatic data processing in the Federal Government. Also included are applicable Office of Management and Budget (OMB) requirements, Federal laws, and results of studies on computer crime conducted by the Department of Justice.

AUDIENCE CATEGORIES

Employees involved in the management, operation, and use of computer systems are divided into five audience categories:

Executives are those senior managers who are responsible for setting agency computer security policy, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the resources and support for the computer security program.

Program and Functional Managers are those managers and supervisors who have a program or functional responsibility (not in the area of computer security) within the agency. They have primary responsibility for the security of their data. This means that they designate the sensitivity and criticality of data and processes, assess the risks to those data, and identify security requirements to the supporting data processing organization, physical security staff, physical facilities personnel, and users of their data. Functional Managers are responsible for assuring the adequacy of all contingency plans relating to the safety and continuing availability of their data.

IRM, Security, and Audit Personnel are all involved with the daily management of the agency's information resources, including the accuracy, availability, and safety of these resources. Each agency assigns responsibility somewhat differently but as a group these persons issue procedures, guidelines, and standards to implement the agency's policy for information security, and to monitor its effectiveness and efficiency. They provide technical assistance to users, functional managers, and to the data processing organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

ADP Management, Operations, and Programming Staff are all involved with the daily management and operations of the automated data processing services. They provide for the protection of data in their custody and identify to the data owners what those security measures are. This group includes such diverse positions as computer operators, schedulers, tape librarians, data base administrators, and systems and applications programmers. They provide the technical expertise for implementing security-related controls within the automated environment. They have primary responsibility for all aspects of contingency planning.

End Users are any employees who have access to an agency computer system that processes sensitive information. This is the largest and most heterogenous group of employees. It consists of everyone from the executive who has a PC with sensitive information to data entry clerks.

TRAINING CONTENT AREAS

There are five training content, or subject matter, areas. The actual selection of the computer security training will depend upon the specific security responsibilities involving duties assigned to individual personnel. The five areas are:

Computer Security Basics is the introduction to the basic concepts behind computer security practices and the importance of the need to protect the information from vulnerabilities to known threats.

Security Planning and Management is concerned with risk analysis, the determination of security requirements, security training and internal agency organization to carry out the computer security function.

Computer Security Policies and Procedures looks at government-wide and agency-specific security practices in the areas of physical, personnel, software, communications, data, and administrative security.

Contingency Planning covers the concepts of all aspects of contingency planning, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all the players involved.

Systems Life Cycle Management discusses how security is addressed during each phase of a systems life cycle (e.g., system design, development, test and evaluation, implementation and maintenance). It addresses procurement, certification, and accreditation.

TRAINING LEVELS

The level of training required in each training, or subject matter, area will vary from general awareness training to specific courses in such areas as Contingency Planning, depending upon the training objectives established by the agency. Note that not every training level is needed for a given audience category or for a given content area.

Awareness training creates the sensitivity to threats and vulnerabilities and the recognition of the

need to protect data, information, and the means of processing them.

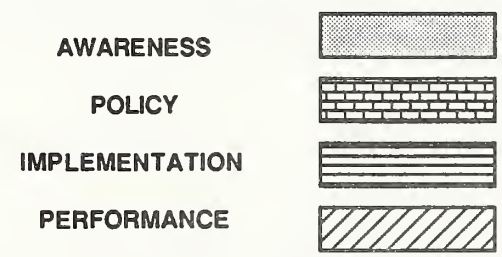
Policy level training provides the ability to understand computer security principles so that executives can make informed policy decisions about computer and information security programs.

Implementation level training provides the ability to recognize and assess the threats and vulnerabilities to automated information resources so that the responsible managers can set security requirements which implement agency security policies.

Performance level training provides the employee with the skill to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

TRAINING MATRIX

Training Area / Audience Category	COMPUTER SECURITY BASICS	SECURITY PLANNING & MGMT.	COMPUTER SECURITY POLICY & PROCEDURES	CONTIN-GENCY PLANNING	SYSTEMS LIFE CYCLE MGMT.
EXECUTIVES					
PROGRAM & FUNCTIONAL MANAGERS					
IRM, SECURITY, AND AUDIT					
ADP MANAGEMENT AND OPERATIONS					
END USERS					



TRAINING FRAMEWORK FOR EACH AUDIENCE CATEGORY

The following pages provide an outline of the training content, or subject matter, areas and the appropriate skills level (e.g., Awareness, Performance, etc.), recommended for each of the five audience categories.

A. AUDIENCE CATEGORY: EXECUTIVES (POLICY MAKERS)

AWARENESS TRAINING

Creates the sensitivity to the threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them.

POLICY LEVEL TRAINING

Provides the ability to understand computer security principles so that executives can make informed policy decisions about the computer security program.

1.0 Computer Security Basics (*Awareness Level*)

1.1 Understanding the threats to and vulnerabilities of computer systems.

- o Definition of terms
- o Major categories of threats, for example: Unauthorized accidental or intentional disclosure, modification, destruction, or delay
- o Threat impact areas
- o Common examples of computer abuse
- o Examples of common system vulnerabilities

1.2 Understanding the roles of various organizational units in assuring adequate security and safety of information resources.

- o Senior Management - the Policy makers
- o End Users and Program or Functional Managers
- o Data Processing Organization
- o IRM, Security and Audit Functions

1.3 Understanding the basic concepts of risk management.

- o Threat and vulnerability assessment
- o Cost/benefit analysis of controls
- o Implementation of cost-effective controls
- o Monitor efficiency and effectiveness of controls

EXECUTIVES (POLICY MAKERS) cont.

2.0 Security Planning and Management (*Policy Level*)

2.1 Deciding on recommendations to organize security program:

- o Setting security policy
- o Establishing roles and delegating authority
- o Assigning responsibility

2.2 Deciding on recommendations for security planning:

- o Setting security goals and objectives:
  - Level of security, and security training requirements
- o Establishing auditing and monitoring functions
- o Authorizing contingency plans
- o Providing resources to meet goals and objectives

2.3 Deciding on recommendations for major risk management projects.

- o Accepting risk as part of doing business
- o Reducing or eliminating risks by employing corrective measures or modifying operations

3.0 Computer Security Policy & Procedures (*Awareness Level*)

3.1 Understanding the need for policies, procedures, and guidance for protection of resources in various areas:

- o - Data and information
- o - Physical
- o - Personnel
- o - Software
- o - Communications
- o - Administrative

4.0 Contingency Planning (*Awareness Level*)

4.1 Understanding the basic concepts of Contingency Planning.

- o Why contingency planning is necessary
- o Who develops the plans
- o The difference between emergency plans, backup plans, and recovery plans

5.0 Systems Life Cycle Management (*Awareness Level*)

5.1 Understanding the basic concepts of Systems Life Cycle Management.

- o Addressing security and internal controls during each phase of automated information system design:

  - Initiation
  - Development
  - Implementation
  - Certification

B. AUDIENCE CATEGORY: PROGRAM/FUNCTIONAL MANAGERS

AWARENESS TRAINING

Creates the sensitivity to threats and vulnerabilities of computer systems and the recognition of the need to protect data, information, and the means of processing them.

IMPLEMENTATION LEVEL TRAINING

Provides the ability to recognize and assess threats and vulnerabilities to automated information resources so that they can set security requirements which implement agency security policies.

PERFORMANCE LEVEL TRAINING

Provides the employee with the skill or ability to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

1.0 Computer Security Basics (*Awareness Level*)

1.1 Understanding the threats to and vulnerabilities of computer systems

- o Definition of terms
- o Major categories of threats, for example: Unauthorized accidental or intentional disclosure, modification, destruction, or delay
- o Threat impact areas
- o Common examples of computer abuse
- o Examples of common system vulnerabilities

1.2 Understanding agency policy and goals for protecting data and information

- o Understanding of agency computer security policies
- o Understanding of agency policy on employee accountability for agency information resources

1.3 Understanding good computer security practices for:

- o Protection of areas
- o Protection of equipment
- o Protection of passwords
- o Protection of files, data
- o Protection against viruses, worms, etc.
- o Backup of data and files
- o Protection of magnetic storage media which contain sensitive information
- o Reporting security violations

1.4 Understanding the roles of various organizational units in assuring adequate security and safety of information resources.

- o Senior Management - the Policy makers
- o End Users and Program or Functional Managers
- o Data Processing Organization
- o IRM, Security and Audit Functions

2.0 Security Planning and Management (*Implementation Level*)

2.1 ADP Security Planning

- o Assigning roles and responsibilities for protection of data which they manage
- o Defining data/systems sensitivity and criticality
- o Determining security requirements
- o Determining security training needs for employees who have access to data and processing equipment
- o Developing and recommending contingency planning requirements
- o Preparing security plans for sensitive systems
- o Determining and requesting resources for security requirements

2.2 Risk Analysis Process

- o Assessing threats and vulnerabilities
- o Performing cost analysis of recommended controls
- o Recommending implementation of controls

PROGRAM/FUNCTIONAL MANAGERS (cont.)

3.0 Security Policies and Procedures (*Implementation Level*)

3.1 Data and Information Security

- o Authorizing access to data, information, and systems
- o Establishing audit trails of records of program and data use, and reviews for irregularities
- o Setting data quality attributes of timeliness, accuracy, completeness, and confidentiality
- o Establishing data transmission verification and validation procedures for data communications
- o Establishing separation of duties rules

3.2 Personnel Security Policies

- o Identifying position sensitivity
- o Initiating employee screening process
- o Taking disciplinary actions

4.0 Contingency Planning (*Performance Level*)

4.1 Assuring adequacy of contingency plans relating to safety and availability of data for which functional manager has primary responsibility:

- o Assigning roles and responsibilities for emergency, backup, and recovery procedures
- o Coordinating emergency procedures with ADP, security, and audit personnel
- o Planning and evaluating backup procedures
- o Planning and providing support in recovery procedures

5.0 Systems Life Cycle Management Processes (*Performance Level*)

5.1 Participating in a management control process that ensures that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications:

- o Evaluating the sensitivity of an application based upon risk analysis
- o Determining security requirements and specifications for acquisitions
- o Evaluating design review and systems test documents to ensure required safeguards are operationally adequate
- o Participating in systems certification and accreditation process

C. AUDIENCE CATEGORY: IRM, SECURITY, AND AUDIT PERSONNEL

AWARENESS TRAINING

Creates a sensitivity to the threats and vulnerabilities of computer systems and a recognition of the need to protect data, information, and the means of processing them.

PERFORMANCE LEVEL TRAINING

Provides the employee with the skill or ability to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

1.0 Computer Security Basics (*Awareness Level*)

1.1 Understanding the threats to and vulnerabilities of computer systems

- o Definition of terms
- o Major categories of threats, for example: Unauthorized accidental or intentional disclosure, modification, destruction, or delay
- o Threat impact areas
- o Common examples of computer abuse
- o Examples of common system vulnerabilities

1.2 Understanding good computer security practices for:

- o Protection of areas
- o Protection of equipment
- o Protection of passwords
- o Protection of files, data
- o Protection against viruses, worms, etc.
- o Backup of data and files
- o Protection of magnetic storage media which contain sensitive information
- o Reporting security violations

1.3 Understanding the roles of various organizational units in assuring adequate security and safety of information resources

- o Senior Management - the Policy Makers
- o End Users and Program or Functional Managers
- o Data Processing Organization
- o IRM, Security and Audit Functions

1.4 Understanding the basic concepts of risk management

- o Threat and vulnerability assessment
- o Cost/benefit analysis of controls
- o Implementation of cost-effective controls
- o Monitoring efficiency and effectiveness of controls

2.0 Security Planning and Management (*Performance Level*)

2.1 Security Planning

- o Developing the agency computer security policy statement for executive action
- o Preparing implementing directives and procedures for computer security policy
- o Developing a computer security program budget
- o Evaluating the effectiveness of the computer security program
- o Identifying security training requirements for managers, operators, and users of agency computer systems

2.2 Risk Analysis

- o Assisting in identifying the roles and responsibilities of all the players in the risk analysis process
- o Integrating vulnerability assessments required by OMB Circulars A-123 and A-130
- o Coordinating and participating in risk analysis studies
- o Assisting in evaluating risk analysis results
- o Recommending corrective actions to ADP and functional managers

2.4 Audit and Monitoring

- o Evaluating the effectiveness of computer security programs
- o Conducting ADP security reviews
- o Participating in verification, validation, testing, and evaluation processes
- o Monitoring ADP systems for accuracy and abnormalities

3.0 Computer Security Policies and Procedures (*Performance Level*)

3.1 Information security

- o Developing, recommending, or performing duties associated with the formulation and implementation of policies and procedures for protecting data and information in areas of:

  - access authorization and authentication
  - designation of sensitive data and applications
  - marking of sensitive data
  - accountability for sensitive data
  - safeguarding and storage of data
  - reproduction of sensitive data
  - transmission of sensitive data
  - destruction of sensitive data
  - reporting of computer misuse or abuse

3.2 Physical security

- o Evaluating and recommending physical security measures which meet the objectives of the agency's security policies in areas of:

  - Building construction
  - Data Processing Centers
  - Physical access control systems
  - Security measures for stand-alone systems and remote terminals
  - Environmental controls
  - Fire safety controls
  - Storage area controls
  - Proper housekeeping procedures

3.3 Personnel Security

- o Developing, recommending, implementing, or evaluating personnel security practices and procedures which support the agency's security policies for:

  - Position sensitivity
  - Employee screening process
  - Security training and awareness

3.4 Software Security

- o Developing, recommending, implementing, or evaluating agency security requirements in the development of agency systems and applications software and configuration management systems for:

  - Programming standards and controls
  - Documentation
  - Change controls
  - Software security systems
  - Audit trails and logging
  - Operating systems security features

3.5 Administrative Security

- o Monitoring administrative procedural controls in each functional area where data and information are received, processed, stored, and disseminated

- o Providing guidance and assisting functional managers in preparation of security plans, including:

  - Investigation of security breaches
  - Reviewing audit trails and logs
  - Reviewing software design standards
  - Reviewing accountability controls in the Data Processing and functional areas

3.6 Communications Security

- o Developing, evaluating, or recommending communications security measures for:
  - Capabilities and limitations of various communications systems
  - Commercial communications protection devices
  - Cryptography

4.0 Contingency Planning (*Performance Level*)

4.1 Providing assistance in the development, coordination, testing, evaluation and implementation of agency contingency plans, as follows:

- o Developing agency response procedures
- o Serving as a team member in responding to an emergency situation
- o Preparing guidelines for determining critical and essential workload
- o Determining backup requirements
- o Advising and assisting in development of procedures for off-site processing
- o Advising and assisting in development or implementation of plans for recovery actions after a disruptive event

5.0 Systems Life Cycle Management (*Performance Level*)

5.1 Developing, recommending, implementing, or reviewing management control processes that ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications:

- o Assisting in evaluation of sensitivity of the application based upon risk analysis
- o Assisting functional management to determine security specifications
- o Performing or assisting in design review and systems test to ensure required safeguards are operationally adequate
- o Performing or assisting in systems certification and accreditation process

D. AUDIENCE CATEGORY: ADP MANAGEMENT, OPERATIONS, and PROGRAMMING STAFF

AWARENESS TRAINING

Creates a sensitivity to the threats and vulnerabilities of computer systems and a recognition of the need to protect data, information, and the means of processing them.

PERFORMANCE LEVEL TRAINING

Provides the employee with the skill or ability to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

1.0 Computer Security Basics (*Awareness Level*)

1.1 Understanding the threats to and vulnerabilities of computer systems

- o Definition of terms
- o Major categories of threats, for example: Unauthorized accidental or intentional disclosure, modification, destruction, or delay
- o Threat impact areas
- o Common examples of computer abuse
- o Examples of common system vulnerabilities

1.2 Understanding good computer security practices for:

- o Protection of areas
- o Protection of equipment
- o Protection of passwords
- o Protection of files, data
- o Protection against viruses, worms, etc.
- o Backup of data and files
- o Protection of magnetic storage media which contain sensitive information
- o Reporting security violations

1.3 Understanding the roles of various organizational units in assuring adequate security and safety of information resources

- o Senior Management - the Policy makers
- o End Users and Program or Functional Managers
- o Data Processing Organization
- o IRM, Security, and Audit Functions

1.4 Understanding the basic concepts of risk management

- o Threat and vulnerability assessment
- o Cost/benefit analysis of controls
- o Implementation of cost-effective controls
- o Monitoring efficiency and effectiveness of controls

2.0 Security Planning and Management (*Performance Level*)

2.1 Establishing a security organizational structure within the data processing environment which implements the agency security program objectives

- o Defining roles and responsibilities for:
  - Data security administrators
  - Computer security officers
- o Interpreting functional management security requirements and applying state-of-the art technology in selection of computer security controls
- o Preparing a computer security program budget for data processing operations
- o Evaluating effectiveness of the computer security program within data processing area
- o Identifying security training requirements for data processing personnel

2.2 Risk Analysis

- o Coordinating and assisting in risk analysis studies
- o Evaluating risk analysis results
- o Recommending and implementing corrective actions to deficiencies identified during risk analysis studies

ADP MANAGEMENT, OPERATIONS, and PROGRAMMING STAFF (cont.)

2.3 Audit and Monitoring

- o Conducting ADP security reviews
- o Coordinating and assisting in the verification, validation, testing, and evaluation process for new or revised systems
- o Assisting in regular reviews of ADP systems for accuracy and abnormalities
- o Maintaining and regularly reviewing both automated and manual logs of:

  - equipment malfunction
  - program aborts
  - magnetic storage media activity
  - program library changes
  - production scheduling and processing
  - input/output activity
  - physical access to data processing areas
  - remote access to computer systems
  - security logs citing security breaches, e.g., unauthorized access attempt

3.0 Computer Security Policies and Procedures (*Performance Level*)

3.1 Information security

- o Developing, recommending, or performing duties associated with the formulation and implementation of policies and procedures for protecting data and information in areas of:

  - access authorization and authentication
  - marking of sensitive data
  - accountability for sensitive data
  - safeguarding and storage of data
  - reproduction of sensitive data
  - transmission of sensitive data
  - destruction of sensitive data
  - reporting of computer misuse or abuse

ADP MANAGEMENT, OPERATIONS, and PROGRAMMING STAFF (cont.)

3.2 Physical security

- o Implementing physical security measures within the data processing environment which meet the objectives of the agency's security policy for:

  - Physical access control systems
  - Security measures for stand-alone systems and remote terminals
  - Environmental controls
  - Fire safety controls
  - Storage area controls
  - Proper housekeeping procedures

3.3 Personnel Security

- o Developing, recommending, implementing, evaluating, or supervising personnel security practices which support the agency's security policy for:

  - Position sensitivity
  - Employee screening process
  - Security training and awareness
  - Recognizing and reporting suspected computer abuse by employees

3.4 Software Security

- o Developing, implementing, evaluating, and monitoring the agency security requirements in the development and implementation of systems and applications software and configuration management systems.

  - Programming standards and controls
  - Documentation
  - Change controls
  - Software security systems
  - Audit trails and logging
  - Operating systems security features
  - System test and evaluation process

3.5 Administrative Security

- o Monitoring administrative and procedural controls in each functional area where data and information are received, processed, stored, and disseminated, for example:

  - Investigating security breaches
  - Reviewing audit trails and logs
  - Reviewing software design standards
  - Reviewing and testing of new or revised application programs
  - Reviewing accountability controls in the Data Processing and functional areas

3.6 Communications Security

- o Developing, implementing, evaluating, or recommending communication security measures in areas of:

  - Capabilities and limitations of various communications systems
  - Commercial communications protection devices
  - Cryptography

4.0 Contingency Planning (*Performance Level*)

4.1 Providing assistance and coordinating the development, testing, and implementation of agency contingency plans:

- o Developing agency emergency response procedures to reduce the probability of a disaster through effective damage control
- o Assuming the leading role in development of the agency contingency plan
- o Identifying and determining cost justification of recovery alternatives available to management
- o Preparing a plan for assignment of resources and responsibilities backing up the processing of the critical workload
- o Advising and assisting functional management in contingency planning
- o Developing, maintaining, and executing disaster recovery plans for resumption of processing after a disruptive event

5.0 Systems Life Cycle Management (*Performance Level*)

5.1 Participating in a management control process that ensures that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications:

- o Assisting in evaluating sensitivity of the application based upon risk analysis
- o Assisting functional management in determining security specifications
- o Performing or assisting in design review and systems test to ensure required safeguards are operationally adequate
- o Performing or assisting in systems certification and accreditation process

E. AUDIENCE CATEGORY: END USERS

AWARENESS TRAINING

Creates the sensitivity to the threats and vulnerabilities of computer systems and provides information on agency policy for protecting data, information, and the means of processing them.

PERFORMANCE LEVEL TRAINING

Provides the employee with the skill or ability to design, execute, or evaluate agency computer security procedures and practices. The objective of this training is that employees will be able to apply security concepts while performing the tasks that relate to their particular positions. It may require education in basic principles and training in state-of-the-art applications.

1.0 Computer Security Basics (*Awareness Level*)

1.1 Understanding the threats to and vulnerabilities of computer systems

- o Definition of terms
- o Major categories of threats, for example: Unauthorized accidental or intentional disclosure, modification, destruction, or delay
- o Threat impact areas
- o Common examples of computer abuse
- o Examples of common system vulnerabilities

1.2 Understanding agency policy and goals for protecting data and information

- o Understanding of agency computer security policies
- o Understanding of agency policy on employee accountability for agency information resources

END USERS (cont.)

1.3 **Understanding good computer security practices for:**

- o Protection of areas
- o Protection of equipment
- o Protection of passwords
- o Protection of files, data
- o Protection against viruses, worms, etc.
- o Backup of data and files
- o Protection of magnetic storage media which contain sensitive information
- o Reporting security violations

2.0 Security Planning and Management (*Awareness Level*)

2.1 **Understanding the roles of various organizational units in assuring adequate security and safety of information resources**

- o Senior Management - the Policy makers
- o End Users and Program or Functional Managers
- o Data Processing Organization
- o IRM, Security, and Audit Functions

2.2 **Understanding the basic concepts of risk management**

- o Threat and vulnerability assessment
- o Cost benefit analysis of controls
- o Implementation of cost effective controls
- o Monitor efficiency and effectiveness of controls

3.0 Computer Security Policies and Procedures (*Performance Level*)

3.1 **Following agency administrative procedures for protection of sensitive data**

- o Designation of sensitive data, applications and systems
- o Marking of sensitive data
- o Accountability for sensitive data
- o Reproduction of sensitive data
- o Transmission of sensitive data
- o Destruction of sensitive data
- o Disclosure of sensitive data
- o Reporting computer abuse

END USERS (cont.)

3.2 Following agency procedures for physical security measures employed to protect data and information:

- o Access controls
- o Fire prevention and protection measures
- o Proper housekeeping procedures
- o Remote terminal protection devices
- o Cryptography device protection

4.0 Contingency Planning (*Performance Level*)

4.1 Following agency emergency procedures by implementing the following:

- o Identifying critical workload
- o Scheduling for backup of critical data
- o Storing and protecting backup files/data
- o Periodically testing with backup files

4.3 Implementing or assisting in implementation of agency recovery procedures:

- o Work scheduling
- o Reconstruction of data bases

5.0 Systems Life Cycle Management (*Awareness Level*)

5.1 Understanding the basic concepts of Systems Life Cycle Management

- o Addressing security and internal controls during each phase of automated information system design:

  - Initiation
  - Development
  - Implementation
  - Certification

CROSS REFERENCES TO EXISTING PUBLICATIONS

1.0 COMPUTER SECURITY BASICS

OMB Circular A-130 "Management of Federal Information Resources"

Privacy Act of 1974, PL 93-579

Computer Fraud and Abuse Act of 1986, PL 99-474

Computer Security Act of 1987, PL 100-235

Computer Crime: Electronic Fund Transfer Systems and Crime, U. S. Dept. of Justice

Computer Crime: Legislative Resource Manual, U.S. Dept. of Justice

FIPS PUB 31, "Guidelines for ADP Security and Risk Management"

FIPS PUB 39 "Glossary for Computer Systems Security"

FIPS PUB 87 "Guidelines for ADP Contingency Planning"

FIPS PUB 112 "Standard on Password Usage"

NBS Special PUB 500-120 "Security of Personal Computer Systems - A Management Guide"

NBS Special PUB 500-153 "Guide to Auditing for Controls and Security - A System Development Life Cycle Approach"

NIST Special PUB 500-166 "Computer Viruses and Related Threats: A Management Guide"

2.0 SECURITY PLANNING AND MANAGEMENT

OMB Circular No. A-123 "Internal Control Systems"

OMB Circular No. A-127 "Financial Management Systems"

OMB Circular No. A-130 "Management of Federal Information Resources"

OMB Bulletin 88-16 "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information"

FIPS PUB 31 "Guidelines for ADP Security and Risk Management"

CROSS REFERENCES TO EXISTING PUBLICATIONS

2.0 SECURITY PLANNING AND MANAGEMENT (cont.)

FIPS PUB 41 "Computer Security Guidelines for Implementing the Privacy Act of 1974"

FIPS PUB 65 "Guideline for Automatic Data Processing Risk Analysis"

FIPS PUB 73 "Guidelines for Security of Computer Applications"

FIPS PUB 94 "Guideline on Electrical Power for ADP Installations"

NBS Special PUB 500-25 "An Analysis of Computer Security Safeguards for Detection and Prevention of Intentional Computer Misuse"

NBS Special PUB 500-33 "Considerations in the Selection of Security Measures of Automatic Data Processing Systems"

NBS Special PUB 500-57 "Evaluation of Computer Security"

NBS Special PUB 500-85 "Executive Guide to ADP Contingency Planning"

NBS Special PUB 500-120 "Security of Personal Computer Systems - A Management Guide"

NBS Special PUB 500-133 "Technology Assessment: Methods for Measuring the Level of Computer Security"

NBS Special PUB 500-153 "Guide to Auditing for Controls and Security: A System Development Life Cycle Approach"

NIST Special PUB 500-166 "Computer Viruses and Related Threats: A Management Guide"

NBSIR 86 "Work Priority Scheme for EDP Audit and Computer Security Review"

OPM 5 CFR PART 930 "Training Requirement for the Computer Security Act"

3.0 COMPUTER SECURITY POLICIES AND PROCEDURES

Privacy Act of 1974, PL 93-579

Federal Manager's Financial Integrity Act of 1982, PL 97-255

Computer Fraud and Abuse Act of 1986, PL 99-474

CROSS REFERENCES TO EXISTING PUBLICATIONS

3.0 COMPUTER SECURITY POLICIES AND PROCEDURES (cont.)

Electronic Communications Privacy Act of 1986, PL 99-508

Computer Security Act of 1987, PL 100-235

OMB Circular No. A-123 "Internal Control Systems"

OMB Circular No. A-127 "Financial Management Systems"

OMB Circular No. A-130 "Management of Federal Information Resources"

FIPS PUB 39 "Glossary for Computer Systems Security"

FIPS PUB 46-1 "Data Encryption Standard"

FIPS PUB 48 "Guidelines on Evaluation of Techniques for Automated Personnel Identification"

FIPS PUB 74 "Guideline for Implementing and Using the NBS Data Encryption Standard"

FIPS PUB 81 "DES Modes of Operation"

FIPS PUB 112 "Standard on Password Usage"

FIPS PUB 113 "Standard on Computer Data Authentication"

NBS Publication List 58 "Federal Information Processing Standards Publications (FIPS PUBs) Index"

NBS Publication List 88 "Computer Science and Technology Publications"

NBS Publication List 91 "Computer Security Publications"

NBS Special PUB 500-61 "Maintenance Testing for the Data Encryption Standard"

NBS Special PUB 500-120 "Security of Personal Computer Systems - A Management Guide"

NBS Special PUB 500-121 "Guidance on Planning and Implementing Computer Systems Reliability"

NBS Special PUB 500-133 "Technology Assessment; Methods for Measuring the Level of Computer Security"

CROSS REFERENCES TO EXISTING PUBLICATIONS

4.0 CONTINGENCY PLANNING

OMB Circular No. A-130 "Management of Federal Information Resources"

Federal Personnel Manual Chapter 732 "Personnel Security"

FIPS PUB 87 "Guidelines for ADP Contingency Planning"

NBS Special PUB 500-85 "Executive Guide to ADP Contingency Planning"

NBS Special PUB 500-134 "Guide on Selecting ADP Backup"

NBS Special PUB 500-156 "Message Authentication Code (MAC) Validation System: Requirements and Procedures"

NBS Special PUB 500-157 "Smart Card Technology: New Methods for Computer Access Control"

NIST Special Publication 500-166 "Computer Viruses and Related Threats - A Management Guide"

5.0 SYSTEMS LIFE CYCLE MANAGEMENT

OMB Circular No. A-123 "Internal Control Systems"

OMB Circular No. A-127 "Financial Management Systems"

OMB Circular No. A-130 "Management of Federal Information Resources"

GAO "Policy and Procedures Manual for Guidance of Federal Agencies, Title II Accounting"

GSA Federal Information Resource Management Regulation (FIRMR), Part 201-30-007 "Determination of Need and Requirements Analysis"

FIPS PUB 38 "Guidelines for Documentation of Computer Programs and Automated Data Systems"

FIPS PUB 64 "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase"

CROSS REFERENCES TO EXISTING PUBLICATIONS

5.0 SYSTEMS LIFE CYCLE MANAGEMENT (cont.)

FIPS PUB 83 "Guideline on User Authentication Techniques for Computer Network Access Control"

FIPS PUB 88 "Guideline on Integrity Assurance and Control in Database Applications"

FIPS PUB 102 "Guideline for Computer Security Certification and Accreditation"

NBS Special PUB 500-105 "Guide to Software Conversion Management"

NBS Special PUB 500-109 "Overview of Computer Security Certification and Accreditation"

NBS Special PUB 500-121 "Guidance on Planning and Implementing Computer Systems Reliability"

NBS Special PUB 500-133 "Technology Assessment: Methods for Measuring the Level of Computer Security"

NIST Special PUB 500-166 "Computer Viruses and Related Threats - A Management Guide"

PCMI and PCIE "Model Framework for Management Control over Automated Information Systems"

☆ U.S.GOVERNMENT PRINTING OFFICE: 1989-261-913/00081

NBS-114A (REV. 2-80)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NIST/SP-500/172	2. Performing Organ. Report No.	3. Publication Date November 1989

4. TITLE AND SUBTITLE

COMPUTER SECURITY TRAINING GUIDELINES

5. AUTHOR(S)

Mary Anne Todd and Constance Guitian

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
(formerly NATIONAL BUREAU OF STANDARDS)
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as Item #6

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 89-600771

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

These guidelines describe what should be the learning objectives of agency security training programs. They focus on what the employee should know, and what they should be able to direct or perform. This allows agencies to design training programs that fit their environments and to clearly state the purpose of the training. Effectiveness can be measured by determining how many of the learning objectives were met.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

ADP Management and operations staff; audience categories; end users; learning objectives; program and functional managers; security awareness; training content areas ; training levels

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

38

15. Price

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, MD 20899