PB84-171339

Guidelines for Development of NASA (National Aeronautics and Space Administration) Computer Security Training Programs

MITRE Corp., McLean, VA. METREK Div

Prepared for

National Aeronautics and Space Administration
Washington, DC

May 83

U.S. Department of Commerce
National Technical Information Service
NTIS

Guidelines for Development of NASA Computer Security Training Programs

Frederick G. Tompkins

May 1983

MTR-83W68

SPONSOR:
NASA
CONTRACT NO.:
NASW-3425
PROJECT NO.:
1915F
DEPT.:
W-27

The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, Virginia 22102

50272-101

REPORT DOCUMENTATION PAGE	1. REPORT NO.	2.	3. Recipient's Accession No. PB84 171339

4. Title and Subtitle

Guidelines for Development of NASA Computer Security Training Programs

5. Report Date

May 1983

6.

7. Author(s)

Frederick G. Tompkins

8. Performing Organization Rept. No.

MTR-83W68

9. Performing Organization Name and Address

The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, VA 22102

10. Project/Task/Work Unit No.

1915F

11. Contract(C) or Grant(G) No.

(C) NASW-3485

(G)

12. Sponsoring Organization Name and Address

National Aeronautics and Space Administration
400 Maryland Avenue, SW
Washington, DC 20546

13. Type of Report & Period Covered

FINAL

14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This report presents guidance for the NASA Computer Security Program Manager and the NASA Center Computer Security Officials as they develop training requirements and implement computer security training programs. NASA audiences are categorized based on the computer security knowledge required to accomplish identified job functions. Training requirements, in terms of training subject areas, are presented for both computer security program management personnel and computer resource providers and users. Sources of computer security training are identified.

17. Document Analysis a. Descriptors

Computer security, ADP security, computer security training requirements

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement: Release Unlimited	19. Security Class (This Report) Unclassified	21. No. of Pages 50
	20. Security Class (This Page)	22. Price

(See ANSI-Z39.18)

See Instructions on Reverse

OPTIONAL FORM 272 (4-77)
(Formerly NTIS-35)
Department of Commerce

ABSTRACT

This report presents guidance for the NASA Computer Security Program Manager and the NASA Center Computer Security Officials as they develop training requirements and implement computer security training programs. NASA audiences are categorized based on the computer security knowledge required to accomplish identified job functions. Training requirements, in terms of training subject areas, are presented for both computer security program management personnel and computer resource providers and users. Sources of computer security training are identified. Recommendations are presented which discuss the need for some type of NASA Headquarters' sponsored computer security training curriculum.

Preceding page blank

ACKNOWLEDGEMENT

The author wishes to thank R. S. Rice of NASA who provided assistance to MITRE during the writing of this report and the following individuals who provided background information: Major V. Marshall, Department of Defense Computer Institute; R. Martian, General Electric Corporation; and D. Fagg, Naval Data Automation Command. The author would also like to thank MITRE associates W. T. Bisignani and J. Sprung for suggestions and review of the final report and M. Bashioum for editorial suggestions and clerical support.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Concluded)

LIST OF ILLUSTRATIONS

1. INTRODUCTION

Training is one of the essential computer security program activities for assuring that NASA (and NASA contractor) personnel acquire and maintain the skills and knowledge to discharge NASA Computer Security Program responsibilities. This report identifies the NASA audiences that require training, the subjects that should be included in a NASA computer security training program, and sources of training available to NASA personnel.

1.1 Background

Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, July 27, 1978, "Security of Federal Automated Information Systems," requires each federal government department and agency to implement a Computer Security Program. In response to OMB Circular A-71, NASA Headquarters issued computer security policy in NASA Management Instruction (NMI) 2410.7, "Assuring the Security and Integrity of NASA Data Processing." NMI 2410.7 states:

> "It is a NASA policy that appropriate steps be taken to assure adequate levels of security and integrity of data processing installations, systems and data to maintain continuity of operations and to minimize the potential for improper use of systems and data."

Guidance for implementing the NASA computer security policy is provided in Appendix J to NASA Handbook 2410.1, "Computer Resources Management." Appendix J provides detailed guidance concerning the mandatory elements of a computer center security program and approaches to implementing the requirements established by the various program elements. Guidance is based on the fundamental premise that it is not possible to have a completely risk-free data processing environment. Therefore, risks must be managed. The personnel charged with management of the security risks in the NASA data processing environment must have reasonable skills and adequate knowledge in both data processing and security. An effective computer security training program can help ensure that computer security officials and computer resource users acquire and maintain the necessary skills and knowledge.

1.2 Objectives of the Computer Security Training Program

The field of computer security encompasses a broad spectrum of subject material impacting the continuity of data processing operations and the security and integrity of systems and data. The overall goal of a NASA Computer Security Training Program is to ensure that all personnel involved or associated with NASA computer resources are provided adequate computer security training. Training should occur as a result of: (1) NASA Headquarters involvement in providing guidelines and requirements for NASA-wide computer security education and training, and (2) Center plans for meeting their respective training requirements.

To meet the overall goal, the following objectives must be achieved:

- All NASA employees should have an awareness of the scope and magnitude of the computer security risks and the potential impacts on NASA computer resources.

- Computer resource users should be able to identify actual and potential threats to and vulnerabilities of application systems.

- Computer security officials should be able to identify, prescribe, and design cost-effective safeguards for applications software and data processing installations.

1.3 Scope of the NASA Computer Security Training Program

The NASA Computer Security Training Program should be designed to provide training to all levels of NASA management, computer security officials, and computer resource users. The content must address all aspects of computer security management; personnel security; security specifications, design review, and system tests; system certification; risk analysis; contingency planning; etc. The training program must also provide for a variety of training formats: lectures, classroom instruction briefings, and seminars/conferences.

1.4 Report Organization

Section 2 presents a discussion of audiences to be trained. Section 3 provides a description of the training areas that should be included in a training program. Section 4 matches training subjects with the NASA audiences. Section 5 presents the various sources of training that are available to NASA personnel. Section 6 provides some considerations for implementing a computer security training program.

2. AUDIENCES TO BE TRAINED

The overall NASA Computer Security Program is designed to ensure that adequate steps are taken to provide a high degree of assurance so that continuity of operations can be maintained and that systems and data have a high degree of integrity. The Program applies to computers used in support of scientific and technical functions as well as those used in support of business and administrative functions. The success or failure of the Program depends, to a significant degree, upon the training provided to all NASA personnel who manage, provide, or use computer resources.

2.1 Classification of Audiences

From a computer security perspective, there are varied populations of NASA personnel who have some type of responsibility for assuring the continuity of data processing operations and/or the integrity of systems and data. The overall management responsibility of each Center's computer security program, for both continuity of operations and systems and data integrity, is vested in the Center Computer Security Official (CSO) and, ultimately, the center management. Continuity of operations involves the DPI manager, computer operations personnel, computer system maintenance personnel, the Facilities Engineer, and the Center Security Official. System and data integrity involves data owners, data custodians, data users, data providers, DPI/Application CSO, audit personnel, programmers/systems analysts, and financial management personnel.

Appendix A provides a recap of the NASA Computer Security Program activities, the individual responsible, and the section of Appendix J, NHB 2410, from which the responsibities were extracted.

It is possible to develop a variety of training classification schema based on the diversity of audiences who should receive some form of computer security training. An approach that provides a useable framework for identifying computer security training requirements is to base training on the extent to which computer security knowledge is required by the affected individual. In other words, does the individual need an across-the-board understanding of computer security to manage computer security program activities, or does the individual require specific knowledge of a security discipline as it applies to his/her job function. This approach, then, indicates that two groupings reasonably encompass all affected NASA personnel: (1) computer security management personnel and (2) computer resource providers and users.

2.2 Computer Security Management Personnel

NASA has a defined computer security management infrastructure to assure that the NASA-wide Computer Security Program is developed, implemented, and maintained in accordance with the letter and the intent of OMB Circular A-71, TM No. 1. The computer security management infrastructure is consistent with the NASA operating philosophy of centralized issuance of policy and guidelines from the Headquarters with detailed procedural implementation at the installation (center). Management responsibility for the NASA Computer Security Program is divided among the NASA Computer Security Program Manager, center management, Center Computer Security Officials, and DPI/Sensitive Application Computer Security Officials.

2.2.1 NASA Computer Security Program Manager

The NASA Computer Program Manager acts as the focal point for computer security program coordination and facilitation within NASA. The program manager develops computer security policy based upon OMB and other applicable federal requirements, provides guidance on implementation of policy, provides guidelines on methods and approaches for implementation of mandatory program activities, and monitors center-level progress.

As the management official responsible for the development, implementation, and operation of the NASA-wide Computer Security Program, the NASA Computer Security Program Manager should be knowledgeable in data processing and security matters. The realm of knowledge required to oversee the program includes the technical as well as the procedural aspects of the specific computer security program areas articulated in OMB Circular A-71, TM No. 1. The areas are:

1. Assignment of responsibility for security at each installation operated by the agency.

2. Coordination of personnel security policies for screening all individuals participating in the design, operation, or maintenance of NASA computer systems or having access to data in NASA computer systems with NASA security officials.

3. Development of a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new computer applications and into any significant modifications to existing computer applications.

4. Establishment of a program for conducting periodic audits or evaluations and recertifying the adequacy of the security safeguards of each operational sensitive application.

5. Coordination of the establishment of policies and responsibilities for assuring that security requirements are included in specifications for the acquisition or operation of computer facilities, equipment, software packages, or related services with NASA procurement management.

6. Assignment of responsibility and providing methodology guidelines for the conduct of periodic risk analyses for each computer installation operated by the agency.

7. Establishment of policies and responsibilities for assuring that appropriate contingency plans are developed and maintained.

2.2.2 NASA Center Management

Top management at each of the NASA centers is responsible for providing a clear definition of the responsibilities and authority of the Center and DPI/Sensitive Application Computer Security Officials. Top management, to effectively discharge its responsibility, should have an understanding of the fundamental computer security problem, the background and scope of OMB and other federal requirements, the current NASA computer security policies, and an overview of the potential impacts of computer fraud and abuse.

2.2.3 Center Computer Security Officials

Each NASA center Computer Security Official (CSO) is responsible for the development, maintenance, and integration of the center computer security program. It is recognized that at the NASA centers, day-to-day responsibilities for operation of the center computer security program may be assigned below the center CSO level. Due to the range in size and number of actual data processing installations (DPIs), the number of CSOs may range from one (a single CSO at a small center) to a number of CSOs at a large center with several DPIs and several sensitive applications. The designated center CSO, who acts as the center focal point for computer security program activities, should have a broad range of knowledge, experience, and/or training in all areas of data processing (hardware, software, facilities, and personnel) and the security field as it applies to a data processing environment.

2.2.4 Data Processing Installation Computer Security Officials

The data processing installation (DPI) Computer Security Official is responsible for the development, implementation, and administration of the DPI Computer Security Program. For those DPIs that have elected to use a Computer Security Working Group, the DPI CSO coordinates the day-to-day activities of the working group. The DPI CSO is the lead person in the performance of risk analysis. He also recommends corrective security measures, enforces compliance with security procedures. In conjunction with the Center Security Office, the DPI CSO investigates computer security violations. Also, the DPI CSO is responsible for providing security training for

DPI personnel. In view of their broad range of responsibilities, DPI CSOs need an extensive exposure to all facets of the computer security field. Detailed knowledge and/or experience is required in the computer security disciplines that pertain to assuring continuity of data processing operations (e.g., physical security, contingency planning).

2.2.5 Sensitive Application Computer Security Officials

The sensitive application computer security offical, in most cases, is the individual who is identified as the data owner. In those instances where there are no clear procedures in effect for assigning data owner responsibility, the DPI CSO may well be the sensitive application CSO.

The sensitive application CSO, or the individual with data owner responsibility, is responsible for assuring the security and integrity of the application system and the associated data. The knowledge required to assure the security and integrity of systems and data includes an overall understanding of the computer security problem, the threats to and vulnerabilities of the application data, the criteria for determining both sensitivity and criticality, and requirements for backing up of data. Also, the sensitive application CSO should have a detailed understanding of the computer security safeguards relative to the planning, development, testing, and operation of new applications.

2.3 Computer Resource Providers and Users

On a day-to-day basis, computer resource providers and users have responsibilities for assuring the continuity of data processing operations and the integrity of data and systems. NASA's implementation of OMB A-71 generally follows the same dichotomy. For example, risk analyses are performed on data processing installations, and sensitive applications are subjected to an evaluation/certification process. This dichotomy provides a useful way to further categorize NASA computer resource providers and users. The computer security knowledge required to assure continuity of operations will differ from the computer security knowledge required to assure the integrity of data and systems. Some job functions will require knowledge in both areas.

2.3.1 Personnel Concerned with Continuity of Operations

The personnel who are charged with assuring continuity of DP operations include the DPI manager, the working group chairperson, computer operations personnel, computer system maintenance personnel, audit personnel, and the facilities engineering personnel.

2.3.1.1 Data Processing Installation (DPI) Manager

The DPI manager has the primary responsibility for assuring that computer resources are available when required by NASA personnel. From a computer security perspective, the DPI manager is responsible for creating a proper environment for security through leadership, participates in the development of management controls, and interacts on computer security matters with the functional user. The DPI manager needs a broad spectrum of computer security knowledge in the areas of risk management, ADP contingency planning, and telecommunications security.

2.3.1.2 Working Group Chairperson

Some NASA DPIs may have elected to assemble a team of personnel to accomplish the computer security program activities. In those instances where such a group is used, the chairperson of the working group typically coordinates the development of the computer security program and ensures that security requirements are met. The knowledge required to accomplish this function is centered around an understanding of the various CSO functions and the approaches to developing computer security plans. In cases where the chairperson is more intimately involved with the day-to-day execution of the computer security program, more specific knowledge would be required in the areas of risk analysis and ADP contingency planning.

2.3.1.3 Computer Operations Personnel

Computer operations personnel who may be assigned as a member of a working group are responsible for recommending methods and procedures to enhance physical and environmental security, contingency planning, data preparation controls, and media controls. Nonworking group personnel should have a general awareness of the computer security problem and know the procedures for reporting security violations.

2.3.1.4 Computer Maintenance Personnel

Computer maintenance personnel are responsible for determining hardware maintenance schedules, providing and maintaining hardware system documentation, and recommending maintenance standards and procedures. Security training should include awareness presentations and instruction in their duties during emergency and contingency operation situations.

2.3.1.5 Audit Personnel

Audit personnel, in general, are responsible for reviewing the adequacy of computer security programs. When audit personnel are members of a computer security working group, they should provide input on data processing controls which support computer security objectives. In their general or computer security committee role, audit personnel require knowledge of computer security problems, risk analysis, contingency planning, and computer security program auditing.

2.3.1.6 Facilities Engineering Personnel

Faciities engineering personnel are responsible for identifying power, air-conditioning, and structural design requirements. Facilities engineer personnel need to have a basic awareness of the environmental concerns of a computer security program under normal operating conditions. They should be knowledgeable in the areas of ADP contingency planning, emergency management, and recovery operations.

2.3.2 Personnel Concerned with the Integrity of Data and Systems

The personnel who are concerned with or have specific responsibilities for assuring the integrity of data and systems include the DPI manager, the working group chairperson, data owners, data users, data providers, data custodians, programmer/

systems analysts, financial management personnel, and audit personnel.

2.3.2.1 DPI Manager

In discharging his/her responsibilities in the area of data and system integrity, the DPI manager needs to provide the security measures required for all applications. The DPI manager should have training in data integrity controls, protection of systems documentation, and programming practices that enhance security. The DPI manager also needs a broad knowledge base in the contingency planning activities to permit systems to recover from short- and long- term interruptions.

2.3.2.2 Working Group Chairperson

The knowledge required by the working group chairperson for assuring data and system integrity is the same as discussed in Section 2.3.1.2 above.

2.3.2.3 Data Owner

The organization having management responsibility for a project or function is referred to as the data owner. The data owner has the primary responsibility for controlling access, modification authority, use, and publication of a specific data element and the degree of data element integrity. The data owner may be a functional user. Functional users are responsible for determining the sensitivity of data used, identifying the level of protection required for source documents, special handling and disposition requirements for output products, and administrative/procedural controls for functional user personnel. Data owners and/or functional users need to have a basic knowledge of the computer security problem, how to identify sensitive applications, how to protect system-related documentation, and alternatives available for backing up sensitive or critical data.

2.3.2.4 Data User

The data user is the organization that uses data for a mission or function. A data user is a custodian (see Section 2.3.2.6) of at least one copy of data being used. Data users must understand why the data being used needs to be protected. Depending on the scope of usage, data owners may be required to participate in identification of sensitive data, security requirements, and back-up requirements.

2.3.2.5 Data Provider

Data providers are organizations that provide data to a DPI in order for the DPI to perform its assigned mission. A data provider is also a custodian and may or may not be a data owner or user. Data providers should have a basic knowledge of why the data requires protection and the general protection requirements of system-associated data.

2.3.2.6 Data Custodian

A data custodian is the organization or organizational element responsible for maintaining the security and integrity of data and software while it is under the control of that organization.

A DPI is frequently a custodian, often for extended periods, of at least one copy of the data. Custodians should have a basic knowledge of sensitive data identification criteria, data integrity, document protection, and back-up requirements and alternatives.

2.3.2.7 Programmer/Systems Analyst

Programmer/systems analyst personnel are responsible for identifying and documenting application systems and associated data security requirements, developing security specifications, programming security controls in application software, and performing software security certification tests. Programmers/systems analysts also need to have an understanding of the security requirements of systems and data back-up and recovery operations.

2.3.2.8 Financial Management Personnel

Financial management personnel, in addition to their potential role as a function user, may be included as part of the computer security working group. In their working group role, financial management personnel will be involved in defining financial management concepts and assisting in the performance of safeguard costs analysis. They should have a basic understanding of financial safeguards, data integrity, and the evaluation/certification of financial management controls.

2.3.2.9 Audit Personnel

In addition to the knowledge required to audit computer security program adequacy discussed in Section 2.3.1.5, audit personnel may be involved in the development of application systems. Responsibilities may only be to assure that the software is auditable upon implementation. It may also involve review/audit of security requirements and specifications and participation in system tests and evaluations. Auditors should have a good base of knowledge concerning the security aspects of system development activities.

3. COMPUTER SECURITY TRAINING SUBJECTS

The overall NASA Computer Security Training Program must meet the training requirements for each of the audiences identified in Section 2. Subject areas should range from general awareness training to specific courses in such areas as risk analysis, and programming practices for application system development.

Seven subject areas have been selected to meet the computer security training needs of NASA personnel. The subject areas were selected, based upon the computer security knowledge required by the various NASA audiences, as discussed in Section 2. The seven subject areas are:

1. Computer Security Awareness
2. Risk Management
3. Computer Security Program Management
4. Security for Sensitive Applications
5. ADP Contingency Planning
6. Telecommunications Security
7. Office Automation Security

3.1 Computer Security Awareness

Training in this subject area should identify the major issues underlying the ADP security problem, such as growing dependency on computers; need for accurate, efficient, and reliable ADP systems; and the need to protect personal, proprietary, classified, or otherwise sensitive information. Also, an overview of relevant cases of computer fraud and abuse should be reviewed to indicate the types of threats to and vulnerabilities of NASA computer resources.

Recommended subjects that should be presented in this area are:

- Overview of the ADP Security Problem
- OMB Circular A-71, TM No. 1 Requirements
- NASA Policy/Guidance
- Overview of Computer Fraud and Abuse

3.2 Risk Management

Training in this subject area should address the steps necessary to conduct a risk analysis at a NASA DPI. Specific subjects should include instruction in defining: (1) the various risks that can impact a DPI, (2) the consequences of occurrence of various risk scenarios, (3) the degree to which risks can be controlled, and (4) the steps that are being, have been, or can be taken to reduce the occurrence, minimize the consequences, or transfer the impact of risks. Recommended subjects which should be included in this training area are:

- Threat and Vulnerability Analysis
- Risk Analysis Methodologies/Approaches
- Risk Reduction Analysis
- Developing/Implementing Risk Management Plans
- Physical Security
- Computer Hardware Security
- Operating Systems Security

3.3 Computer Security Program Management

This training should cover the assignment of responsibilities and authority of those NASA personnel specifically charged with management of the NASA-wide Computer Security Program and center and DPI computer security plans. Instruction should be provided on how to develop, implement, maintain, and audit computer security programs. Also included should be guidance on the NASA Personnel Security Program for NASA-related positions. Recommended subjects which should be included in this area are:

- CSO Responsibilities
- Developing, Implementing, and Maintaining Computer Security Plans
- Personnel Security/Clearances
- Auditing Computer Security Plans

3.4 Security for Sensitive Applications

This training area should address the management and technical aspects involved in establishing a management control process to assure that appropriate administrative, physical, and technical safeguards are built into all existing and new applications as well as modifications to existing applications. Specific instruction should be devoted to identifying sensitive applications, security planning for applications, developing security specifications, programming practices, and system tests and evaluations. Requirements and approaches for certifying and recertifying security controls in applications should also be addressed.

Recommended subjects which should be included in this training area are:

- Criteria for the Identification of Sensitive Applications
- Software Life Cycle and Security
- Data Integrity

- Document Protection
- Defining Application Security Requirements
- Developing Application Security Specifications
- Programming Practices for Sensitive Applications
- System Test & Evaluation
- Certification of Sensitive Applications
- Recertification Requirements and Approaches

3.5 ADP Contingency Planning

This training area should focus on the need for and activities related to the development and maintenance of plans for assuring the continuity of data processing operations. Subjects to be included under this category should address the criteria and approaches for defining critical applications, alternative backup strategies, and the selection of an alternate data processing operations site. Instruction should include a discussion of the planning steps involved in emergency response, backup operations, and recovery activities. Various methods for testing plans should also be discussed. Recommended subjects which should be included in this training area are:

- The Relationship Between Risk Analysis and Contingency Planning
- Identifying Critical Applications
- Selection of a Backup Strategy
- Planning for Emergency Response
- Planning for Backup Operations
- Planning for Recovery Operations
- Documenting the Contingency Plan
- Testing the Contingency Plan

3.6 Telecommunications Security

This training area should provide a discussion of the security requirements for the various types of communications supporting computer resources. Included should be an overview of the penetration techniques and threats to and vulnerabilities of the telecommunications system. Also, various safeguards, including encryption, should be addressed.

Recommended subjects to be included in this training area are:

- Terminal Security
- Network Security
- Encryption

3.7 Office Automation Security

Training in this area should stress the security problems and potential safeguards for office automation systems. In general, discussions should include physical security, user security practices, system security controls, backup, and security management.

Recommended subjects to be included in this training area are:

- Workspace Security
- Data Security
- Back Up
- Electronic Mail Security

4. PROPOSED TRAINING FOR NASA PERSONNEL

The actual selection of the computer security training course will depend upon the specific computer security duties assigned to individual NASA personnel. The computer security subjects that have been matched to various NASA audiences are intended to be used as general guidelines in developing and implementing center-level computer security training programs.

All NASA personnel should receive initial and periodic computer security awareness briefings. Personnel charged with the managment of the NASA-wide and Center computer security programs should receive training in all facets of computer security. Personnel who are primarily responsible for assuring continuity of operations should receive training in risk management and ADP contingency planning. Personnel responsible for assuring the integrity of systems and data should receive training in security for applications and some aspects of ADP contingency plans. More detailed guidance on recommended minimum and optional subjects is presented in Figure 4-1.

Figure 4.1

Proposed Training Subjects for NASA Personnel

Training Program Content	Computer Security Management Personnel					Personnel Responsible for Continuity of Operations						Personnel Responsible for Systems Data Integrity								
	NASA Computer Security Program Mgr	Center Management	Center Computer Security Official	DPI Computer Security Official	Sensitive Application Computer Security Off.	DPI Manager	Working Group Chairperson	Computer Operations Personnel	Computer System Maintenance Personnel	Audit Personnel	Facilities Engineer	DPI Manager	Working Group Chairperson	Data Owner	Data User	Data Provider	Data Custodian	Programmer/Systems Analyst	Financial Management Personnel	Audit Personnel
I. Computer Security Awareness																				
• ADP Security Problem	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
• OMB A-71, TM #1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
• NASA Policy Guidance	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
• Computer Fraud & Abuse	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
II. Risk Management																				
• Threat Vulnerability Anal.	●	○	●	●	●	●				○	●									
• Risk Analysis Methodology	●	○	●	●	●	●				●	○									
• Risk Reduction Analysis	●	○	●	●	●	●				●	●									
• Developing Risk Mgmt Plans	●	○	●	●		●	○			○										
• Physical Security	●		●	●		●				○	○									
• Hardware Security	●		●	●		●				○										
• Operating Systems Security	●		●	●		●				●										
III. Computer Security Program Management																				
• CSO Responsibilities	●	●	●	●	●	●	●			●		●	●							●
• Developing Com Scty Plans	●	●	●	●	●	○	●			●		○	●							●
• Personnel Sct Clearances	●	○	●	●	●	●	○			●		●	○							●
• Auditing Comp Scty Plans	●	○	●	○	○		○			●			●							●
IV. Security for Sensitive Appl.																				
• Ident. of Sensitive Appl.	●	○	●	●	●							○		●	●	●	●	●	●	●
• Applications S W Safeguards	●		●	○	●							○		●	●		○	●	●	●
• Data Integrity	●		●		●							●		●	●	○	●	●	●	●
• Document Protection	●		●		●							●		●	●	●	●	●		●
• Security Requirements	●		●		●							○		●				●		●
• Security Specifications	●		●		●							○		○				●		●
• Programming Practices	●		●		●							●						●		●
• System Test & Evaluation	●		●		●							○						●		●
• Certification	●	○	●		●							○		○				●	●	●
• Recertification	●		●		●							○		○				●	●	●
V. ADP Contingency Planning																				
• Risk Analysis	●	○	●	●	●	●				○		●								●
• Identifying Critical Appl.	●		●	●	●	●				●		●		●	○	○	●	○		●
• Backup Strategy Selection	●		●	●	●	●				○		●		●	○		●	●		○
• Emergency Response Plan	●		●	●	○	●		●	●	○	●	●						●		○
• Backup Operations Plan	●		●	●	○	●		●		○	●	●						●		○
• Recovery Plan	●		●	●	○	●			●	○	●	●						●		○
• Testing	●		●	●	●	●		●		●	●	●		○	○	○	○	●		●
VI. Telecommunications Security																				
• Terminal Securty	●	○	●	●	●	●				●	○							○		●
• Network Security	●		●	●	○	●				●								○		●
• Encryption	●		●	●		○				○								○		○
VII. Office Automation Security																				
• Work Space Security	●	○	●	○	●	○				○	●	○		○	●					●
• Data Security	●		●	●	●	●				●		●		●	●	●	●	○	●	●
• Backup	●		●	○	●	●				○		●		●	●		●	○		○
• Electronic Mail Security	●	○	●	○	●	○				○		●								○

Legend:
● Minimum Training Requirement
○ Optional Subject

Preceding page blank

5. SOURCES OF COMPUTER SECURITY TRAINING

Several sources of computer security training are available to NASA personnel. The Department of Defense, Department of Agriculture, and the Office of Personnel Management are the primary federal government agencies offering computer security courses. Computer security courses may be included in the educational programs offered by most of the major computer and software vendors. Some colleges and universities are including a course in computer security in their computer science and/or security management curriculum. Professional societies such as the Association for Computing Machinery (ACM), the Institute of Internal Auditors, the EDP Auditors Association, and The American Society of Industrial Security periodically offer workshops and seminars on computer security. A number of conferences such as the National Computer Conference, the Federal DP Exposition, and WESCON often include individual sessions or panel discussions on a variety of computer security subjects. Computer-oriented publications such as COMPUTERWORLD, DATAMATION, and INFO SYSTEMS usually include a calendar of various courses and conferences.

5.1 Points of Contact for Government Training Sources

The agencies identified below offer periodic courses on computer security.

5.1.1 Department of Defense Computer Institute (DoDCI)

DoDCI is a part of the National Defense University and offers two courses of potential value to NASA personnel; (1) Managing Automated Information System Resource Protection and (2) The Privacy Act and The Manager.

The Managing Automated Information System Resource Protection course is designed to develop an understanding of computer and computer-based information system protection problems and presents a systematic approach to the development and/or enhancement of a computer security progam. The concepts of risk management and the trade-off analysis for the selection of safeguards are developed. Implementation and operation of a computer security program are also discussed. An extensive case study is included.

The Privacy Act and The Manager course directs its efforts towards the major requirements of the Privacy Act and the impact of those requirements on the information processing environment. Instruction will place into perspective the problems of data accuracy, privacy, confidentiality, and responsibility. Students are offered a systematic approach to solving these problems. A case study is included.

Non-Department of Defense agencies are invited to nominate personnel for DoDCI resident courses on a space-available basis. A minimal fee is assessed. Nominations should be submitted using Standard Form 182 or Option Forms 170 or 37.

Contact: DoDCI Registrar
Washington Navy Yard (Bldg. 175)
Washington, D.C. 20374
(202) 433-3391

5.1.2 U.S. Army Logistics Management Center (ALMC)

The ALMC course, Security in Automated Systems, runs for eight days, covering major aspects of computer security. It specifically describes minimum security requirements for Army automated systems. The course combines formal classroom lectures with individual research and group study. Guest speakers are invited to provide instruction in their particular area of expertise. The ALMC course is open to military officers, senior noncommissioned officers, and civilian personnel who are involved in automation security. Information on this course can be obtained from:

Commandant, ALMC
DRXMC-A-R
Fort Lee, Virginia 23801
(804) 734-1277

5.1.3 Army Institute for Professional Development

The Army sponsors an extensive correspondence course program administered by the Army Institute for Professional Development. The courses and subcourses offered cover a wide range of subjects, including one entitled Basic Principles of ADP Management, which includes some automation security information. A listing of courses is contained in DA PAM 351-20-8, U.S. Army Institute Administration Correspondence Course Catalog. This pamphlet and information concerning enrollment is available from:

Army Institute for Professional Development
U.S. Army Training Support Center
Newport News, Virginia 23628

5.1.4 Office of Personnel Management

The OPM ADP Management Training Center in Washington, D.C. offers a three-day course entitled, Security and Privacy. The course is primarily conducted by guest faculty who have current experience in security and privacy operations. Case studies and problems are utilized in addition to lecture material. Topics addressed in the course include; History of Information Systems Privacy, Legal Environment, Total Systems Security, Environmental Security, Installation Security, Software Security, and Cost-Benefit Analysis.

OPM may offer additional courses through their regional training offices. Information on the courses described above and the location of the regional training offices is available from:

Office of Personnel Management (OPM)
The ADP Management Training Center
1900 E Street, N.W.
Washington, D.C. 20415
(202) 632-5650

5.1.5 Graduate School, U.S. Department of Agriculture

The Graduate School course, Computer Systems Security: A Management Approach to Countering Computer Fraud, is presented in Washington, D.C. This five-day seminar is designed to benefit top managers as well as those with direct responsibility for the protection and effective use of ADP assets. It should be taken by persons involved in setting up organizational policy, developing standards, preparing security plans, performing risk analyses, and developing ADP facility back-up and contingency plans. Arrangements can be made for on-site presentation as well.

For additional information contact:

Graduate School
U.S. Department of Agriculture
Capital Gallery
600 Maryland Avenue, S.W.
Room 106
Washington, D.C. 20024
(202) 447-7124

5.2 Points of Contact for Professional Organizations

The organizations listed on the following pages offer conferences, seminars, and workshops that usually include computer security subjects.

5.2.1 Institute of Internal Auditors (IIA)

IIA offers training primarily oriented to the needs of auditors. The most comprehensive training is provided at the Computer Audit, Control, and Security Conference. The conference is presented annually and covers the state-of-the-art in computer security and auditing developments.

Additional information is available from:

Institute of Internal Auditors, Inc.
5500 Diplomat Circle
Orlando, Florida 32810
(305) 830-7600

5.2.2 EDP Auditors Association (EDPAA)

EDPAA sponsors a yearly national conference and periodic regional seminars that usually include sessions on computer security. The EDP Auditors Foundation for Education and Research publishes a quarterly journal and various studies such as, "Control Objectives - 1980." Also, major metropolitan areas have local chapters that hold monthly meetings, usually with a guest speaker.

Additional information can be obtained from:

EDP Auditors Association
373 South Schmale Road
Carol Stream, Illinois 60187
(312) 653-0950

EDP Auditors Foundation
P.O. Box 2051
Winter Park, Florida 32790
(305) 628-5515

5.2.3 Computer Security Institute (CSI)

CSI sponsors a yearly conference and publishes the newsletter, *Computer Security*. CSI offers computer security courses, periodically, in various geographic areas. Courses may also be contracted for on-site presentation.

Additional information can be obtained from:

Computer Security Institute
43 Boston Post Road
Northborough, Massachusetts 01532
(617) 845-5050

5.2.4 American Society for Industrial Security (ASIS)

ASIS is a professional membership society of security practitioners. ASIS, through its Computer Security Committee, sponsors an annual computer security workshop. Sessions on computer security topics are presented as part of the Society's annual seminar and exhibits.

Additional information can be obtained from:

American Society for Industrial Security
1655 N. Fort Myer Drive
Suite 1200
Arlington, Virginia 22209
(703) 522-5800

5.3 Newsletters

A number of newsletters are currently published which are devoted primarily to the field of computer security.

5.3.1 EDPACS - The EDP Audit, Control and Security Newsletter

EDPACS is published monthly. It is primrily oriented to EDP auditors and their responsibilities for auditing EDP systems. Many, if not most, articles are of value to computer security practitioners.

Additional information can be obtained from:

Editor EDPACS (regarding editorial matters)
Automation Training Center, Inc.
11250 Roger Bacon Drive, Suite 17
Reston, Virginia 22090

Publications Secretary (for
circulation/subscription information)
The Institute of Internal Auditors, Inc.
249 Maitland Avenue
Altamonte Springs, Florida 32701
(305) 830-7600

5.3.2 "Computer Security"

"Computer Security" is published every other month by the Computer Security Institute. Circulation is restricted to members of the institute and is not sold by subscription. (Refer to Section 5.2.3 for contact information).

5.3.3 The "Security Management Report" (SMR)

SMR is published monthly and is oriented to data processing protection personnel. SMR includes articles and checklists on various aspects of computer security. Additional information can be obtained from:

Security Management Report
185 E. Garfield Avenue
Pomona, California 91767
(714) 622-3662

5.4 Training Films

The organizations identified below offer training films which are specifically directed at computer security or include computer security material. Most films are available on a preview, rental, or purchase basis.

Catalogs can be obtained by contacting the following offices:

- ADVANCED SYSTEMS, INC.
  1777 North Kent Street
  Suite 703
  Arlington, Virginia 22209
  (703) 524-2277

- DELTAK, INC.
  East/West Technological Center
  1751 West Diehle Road
  Naperville, Illinois 60566
  (800) 532-7686

- EDUTRONICS (McGraw-Hill)
  1750 K Street, N.W.
  Suite 1170
  Washington, D.C. 20006
  (202) 463-1721

- MTI Teleprograms
  3710 Commercial Avenue
  Northbrook, Illinois 60062
  (800) 323-5343

- Vision Associates
  85 Scollard Street
  Toronto, Canada M5R1G4
  (416) 960-1636

- Visucom Video Arts
  P.O. Box 5472
  Redwood City, California 94063
  (800) 222-4002
  (415) 364-5566 (California only)

6. NASA COMPUTER SECURITY TRAINING PROGRAM - IMPLEMENTATION CONSIDERATIONS

The responsibility for the implementation of the NASA Computer Security Training Program is shared by NASA Headquarters and the NASA Centers. NASA Headquarters, in addition to being responsible for the overall management of the program, should identify a generic training program for Center, DPI, and Application CSOs. A CSO computer security course should address computer security program management and provide an overview of the various activities attendant to developing and operating a computer security program at a NASA center.

The NASA Computer Security Program Manager will work with the Agency Training Office to determine what computer security training should be offered on an agency-wide basis. Consideration should be given to reviewing any existing NASA-wide sponsored training in the areas of data processing and data processing management to determine where inclusion of computer security training would be appropriate.

Each of the NASA Center CSOs should identify the Center audiences requiring computer security training, identify potential sources, and develop a training schedule in coordination with each center's training office.

APPENDIX A

COMPUTER SECURITY PROGRAM ACTIVITIES AND RESPONSIBLE NASA INDIVIDUAL

ACTIVITY	RESPONSIBILITY	REFERENCE*
Identification of a sensitive application	Data Owner	Section 502 para 4a
Comprehensive list of sensitive applications	DPI CSO	Section 502 para 4b
Initial responsibility for determination of sensitive applications	DPI CSO	Section 502 para 4b
Assures sound control is maintained over sensitive application software	DPI CSO	Section 502 para 4b
Assures sound definition is made of sensitive and nonsensitive applications	Center CSO	Section 502 para 4c
Defines responsibilities and authority of each center CSO	Center Mgmt	Section 502 para 4d
Backup of data	User or Provider of Data Shared with DPI (Mgmt)	Section 504 para 3
DPI personnel security clearances & procedures	DPI Manager	Section 507 para 2

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

ACTIVITY	RESPONSIBILITY	REFERENCE*
Primary auth & resp for control access, modification, authority, use of and publication of a specific data element and degree of data element integrity	Data Owner	Section 508 para 2
Organization responsible for maintaining security and integrity of data (including software) while under its control	Data Custodian	Section 508 para 2
Organization that uses data for a mission or function	Data User	Section 508 para 2
Organization that provides data to DPI	Data Provider	Section 508 para 2
Ultimate responsibility for centers' Computer Security Program - Develops awareness of security requirements - Maintains documentation and reports involving center CSP - Interfaces with other centers/Headquarters	Center CSO	Section 509 para 3a
Coordinates development of security program	W/Group Chairperson	Section 508 para 3b

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

ACTIVITY	RESPONSIBILITY	REFERENCE*
Ensures security requirements are met	W/Group Chairperson	Section 508 para 3b
Resolves conflicts		
Coordinates day-to-day activities of the Working Group	DPI CSO	Section 509 para 3c
Lead person in performance of vulnerability, threat, risk analysis		
Recommends corrective measures		
Administers DPI Computer Security Program CPS		
Provides security training		
Enforces compliance with security procedures		
Investigates security violations		
Creates proper environment for security	DPI Manager	Section 509 para 3d
Participates in development of mgmt controls		
Interacts with function users		
Determines sensitivity of data used	Functional User	Section 509 para 3e

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

ACTIVITY	RESPONSIBILITY	REFERENCE*
Identifies source documents under user controls and level of protection required	Functional User	Section 509 para 3e
Determines report utilization, special handling, and disposition		
Determines essential controls for personnel		
Processes personnel security clearances for ADP sensitive positions	Center Security Officer (CSO)	Section 509 para 3f
Recommends physical security controls		
Identifies power/AC requirements	Facilities Engineer	Section 509 para 3g
Establishes structural design requirements		
Monitors accuracy cnecks	Audit Personnel	Section 509 para 3h
Recommends data integrity Controls		
Recommends controls for fraud and computer abuse		
Recommends data processing controls		
Recommends:	Computer Operations Personnel	Section 509 para 3i

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

ACTIVITY	RESPONSIBILITY	REFERENCE*
- Methods & procedures - Emergency (contingency) plans - System backup requirements - Data processing controls - Media controls	Computer Operations Personnel	Section 509 para 3i
Recommends/Develops: - System development procedures - Programming standards and practices - Documentation requirements - Software certification procedures - Test and evaluation procedures	Programmer/ Systems Analyst	Section 509 para 3j
Determine maintenance schedules Provide H/W documentation Recommend maintenance standards and procedures	Computer System Maintenance Personnel	Section 509 para 3k

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

ACTIVITY	RESPONSIBILITY	REFERENCE*
Define financial mgmt controls	Financial Management Personnel	Section 509 para 31
Perform safeguard cost analysis		

*Appendix J, NASA Handbook (NHB) 2410.1, Computer Resources Management.

APPENDIX B

BIBLIOGRAPHY

Air Force Computer Security Program Office (AFDSDC/SCP), 31 July 1982.

Department of the Army, Army Automation Security Program Technical Bulletin, (DRAFT).

Department of the Navy, Department of the Navy Automatic Data Processing Security Program, OPNANINST 5239.1A, August 3. 1982.

Mastbrook, David W., Guidance for Developing a Five Year Plan for the NASA Computer Security Program, WP82W00489, The MITRE Corporation, McLean, Virginia, August 1982.

NASA Handbook (NHB) 2410, Computer Resources Management.

NASA Management instruction (NMI) 2410.7, Assuring Security and Integrity of NASA Data Processing.

National Defense University, Department of Defense Computer Institute (DoDCI), Course Information, November 1982.

OMB Circular A-71, Transmittal Memorandum No. 1, July 27, 1978.

U.S. Air Force, Air Force Computer Security Program "Training Plan" for the Air Force Data Processing Security (ADPSEC) Project, (DRAFT).

U.S. Army Logistics Management Center, Program of Instruction for Security in Automated Systems Course (SAS), ALM-68-0297-POI, March 1981.

U.S. Department of Agriculture, Career Planning and Development Programs, Computer Sciences 1982-83, Graduate School, USDA.