PB91-187781

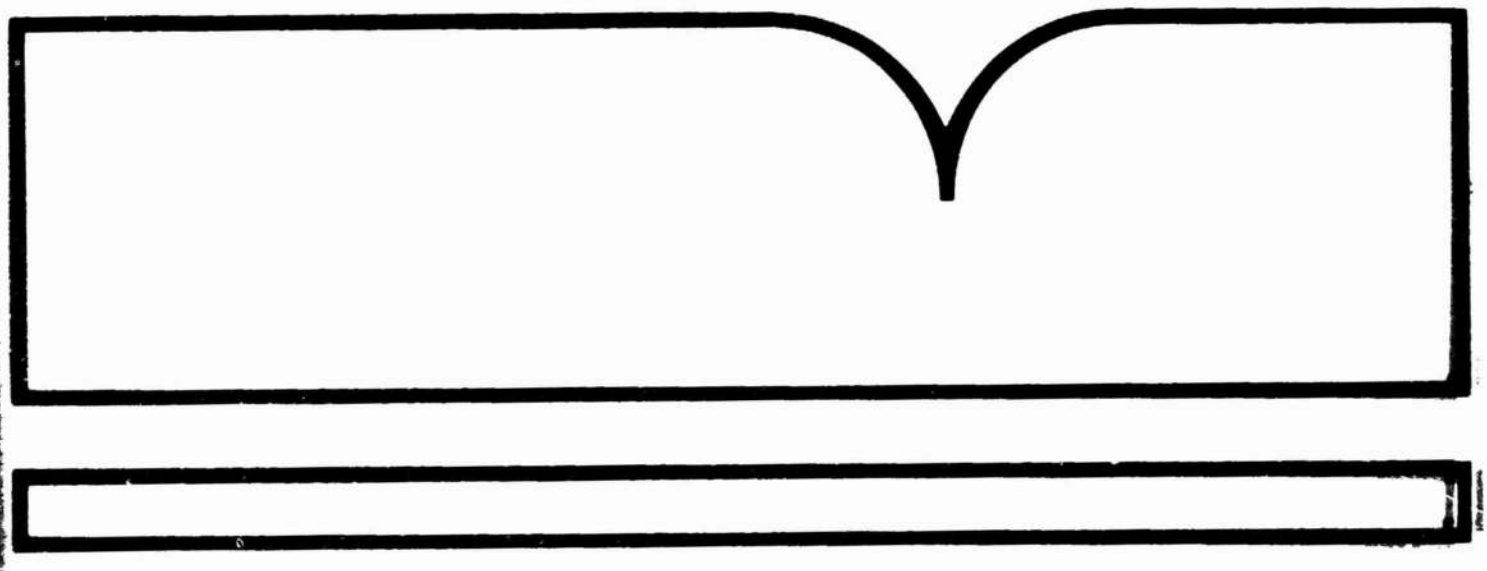
# National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook

(U.S.) National Inst. of Standards and Technology, Gaithersburg, MD

Prepared for:

National Aeronautics and Space Administration, Washington, DC

Mar 91



PB91-187731

NISTIR 4518

# National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook

**Edward Roback**
**NIST Coordinator**

**U.S. DEPARTMENT OF COMMERCE**
**National Institute of Standards and Technology**
**Gaithersburg, MD 20899**

**U.S. DEPARTMENT OF COMMERCE**
**Robert Mosbacher, Secretary**
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
**John W. Lyons, Director**

NIST

NIST-114A
(REV. 3-90)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

# BIBLIOGRAPHIC DATA SHEET

1. NISTIR 4518

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
MARCH 1991

4. TITLE AND SUBTITLE

National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook

5. AUTHOR(S)

Edward Roback, NIST Coordinator

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Reprinted by permission of National Aeronautics and Space Administration, Washington, DC 20546

10. SUPPLEMENTARY NOTES

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.)

The National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook provides NASA's overall approach to automated information systems security including discussions of such aspects as: program goals and objectives, assignment of responsibilities, risk assessment, foreign national access, contingency planning and disaster recovery, awareness training, procurement, certification, planning, and special considerations for microcomputers.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

accreditation; ADP security; automated information system security; certification; computer security; contingency plan; risk assessment; telecommunications security

13. AVAILABILITY

- [X] UNLIMITED
- [ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).
- [ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.
- [X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
106

15. PRICE
A06

ELECTRONIC FORM

NISTIR 4518

# National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook

**Edward Roback**
**NIST Coordinator**

**U.S. DEPARTMENT OF COMMERCE**
**National Institute of Standards and Technology**
**Gaithersburg, MD 20899**

**March 1991**

**U.S. DEPARTMENT OF COMMERCE**
**Robert A. Mosbacher, Secretary**
**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**
**John W. Lyons, Director**

## Forward

This National Institute of Standards and Technology Interagency Report (NISTIR) presents the National Aeronautics and Space Administration's (NASA) Automated Information Security Handbook. The Handbook provides NASA's overall approach to automated information systems security including: program goals and objectives, assignment of responsibilities, risk assessment, foreign national access, contingency planning and disaster recovery, awareness training, procurement, certification, planning, and special considerations for microcomputers.

Note that Chapters seven through nine, which deal exclusively with the protection of classified information, have not been included in this publication. Such requirements are well known and are readily available in other forms.

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this Handbook. However, as this material may be of use to other organizations, the report is being reprinted by NIST to provide for broad public dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the NASA's Information Resources Management Office of the Office of Management for their kind permission to publish this report.

Questions regarding this publication should be addressed to the Associate Director for Computer Security, National Computer Systems Laboratory, Building 225, Room B154, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161, telephone: (703) 487-4650.

NHB 2410.9
SEPTEMBER 1990

# NASA

# AUTOMATED INFORMATION SECURITY HANDBOOK

INFORMATION RESOURCES MANAGEMENT OFFICE
OFFICE OF MANAGEMENT
NATIONAL AERONAUTICS & SPACE ADMINISTRATION

Preceding page blank

# NASA AUTOMATED INFORMATION SECURITY HANDBOOK

## PREFACE

Public Law and National Policy require Federal agencies to establish automated information systems security programs to assure adequate levels of security for all agency automated information systems, whether maintained in-house or commercially.

Automated information systems security is becoming an increasingly important issue for all NASA managers. Rapid advancements in computer technology and the demanding nature of space exploration and space research have made NASA increasingly dependent on computers to store, process, and transmit vast amounts of mission support information. In many cases, automated processes are an integral function that directly contributes to the success of a NASA mission. In today's electronically-based society, the practice of effective computer security management principles is an inherent function of good business and good professional practice.

The computer security management processes covered by this Handbook exemplify our efforts to assure that scientific missions and business functions are carried out in an accurate, safe, accountable, and efficient manner. This Handbook, in addition to NMI 2410.7, "Assuring the Security and Integrity of NASA Automated Information Resources," provides consistent policies, procedures, and guidance to assure that an aggressive and effective program is developed, implemented, and sustained. The provisions of this Handbook apply to all NASA organizations and NASA support contractors. Generally excluded are contractor or research facility automated information resources not under direct NASA management control.

This Handbook is intended primarily for use by Program Office Computer Security Managers (PO-CSM's) at Headquarters and Center Computer Security Managers (CCSM's) at field centers; however, it has been structured to allow anyone from senior management to technical support personnel to quickly understand the overall concepts and their personal relationship to the program. The intention of providing implementation flexibility in the guidance portions is to encourage the exercise of sound judgement by those closest to a problem. PO-CSM's and CCSM's are expected to apply common sense in determining appropriate variations and exceptions that may become necessary in specific computing environments.

This Handbook is issued in loose-leaf form and will be revised by page changes. Comments and suggestions concerning this Handbook should be addressed to the NASA Automated Information Security Program Manager, Code NTD, NASA Headquarters, Washington, DC 20546.

Associate Administrator
for Management

DISTRIBUTION:
SDL 1(SIQ)

# TABLE OF CONTENTS


| Paragraph | | Page |
|---|---|---|
| | CHAPTER 1. PROGRAM OVERVIEW | |
| 100 | Introduction | 1-1 |
| | a. Management Issue | 1-1 |
| | b. Value of Information and Computing Resources | 1-1 |
| | c. Life-Cycle Phases | 1-1 |
| | d. History | 1-1 |
| | e. References | 1-2 |
| | f. Terminology | 1-3 |
| 101 | Purpose | 1-3 |
| 102 | Organizational Scope | 1-3 |
| 103 | Systems Covered | 1-4 |
| 104 | Exceptions | 1-4 |
| 105 | NASA Computer Systems Environment | 1-4 |
| 106 | Importance of an Effective Computer Security Program | 1-5 |
| | a. Public Image | 1-5 |
| | b. Increasing Incidents | 1-5 |
| | c. Management Priority | 1-5 |
| 107 | NASA Automated Information Security Program Background | 1-5 |
| | a. Initial Policy | 1-5 |
| | b. Initial Handbook | 1-5 |
| | c. Summary of Other Milestones | 1-6 |
| 108 | Origin of National Policy | 1-6 |
| | a. National Organizations | 1-6 |
| | b. National Documents | 1-6 |
| | CHAPTER 2. PROGRAM ORGANIZATION AND MANAGEMENT | |
| 200 | Introduction | 2-1 |
| 201 | Management Philosophies | 2-1 |
| | a. Integration | 2-1 |
| | b. Decentralization | 2-1 |
| | c. Perfection | 2-1 |

| Paragraph | | Page |
|---|---|---|
| 202 | NASA Automated Information Security Program Goal and Objectives | 2-2 |
| | a. Goal | 2-2 |
| | b. Objectives | 2-2 |
| 203 | Program Elements | 2-3 |
| | a. Basic Elements | 2-3 |
| | b. Sustaining Program Effectiveness | 2-5 |
| 204 | NASA Computer Security Policy | 2-5 |
| 205 | Headquarters Roles and Responsibilities | 2-6 |
| | a. Overview | 2-6 |
| | b. Multidisciplinary Coordination | 2-6 |
| | c. NASA Automated Information Security Program Manager | 2-6 |
| | d. Headquarters Program Offices | 2-9 |
| | e. Other Headquarters Offices | 2-10 |
| 206 | Individual Responsibilities for Computer Security | 2-10 |
| 207 | Program Organizational Structure | 2-12 |
| 208 | Management Review and Compliance Assurance Process | 2-12 |
| | a. Headquarters Reviews | 2-14 |
| | b. Center Reviews | 2-14 |
| | c. DPI Reviews | 2-14 |
| | CHAPTER 3. CENTER AND DPI REQUIREMENTS | |
| 300 | Center Requirements | 3-1 |
| | a. Designation of Authorities | 3-1 |
| | b. CCSM Responsibilities | 3-1 |
| | c. Identifying DPI's | 3-2 |
| | d. Identifying Additional Entities | 3-4 |
| 301 | DPI Requirements | 3-4 |
| | a. Designation of Authorities | 3-4 |
| | b. DPI-CSO Responsibilities | 3-4 |
| 302 | Management Process | 3-5 |
| | a. Risk Assessments | 3-6 |
| | b. Certifying Requirements | 3-6 |

| Paragraph | | Page |
|---|---|---|
| | c. Personnel Screening | 3-6 |
| | d. Access Protection and Accountability | 3-6 |
| | e. Compliance Assurance | 3-6 |
| | f. Contingency and Disaster Recovery Plans | 3-7 |
| | g. Approval of Methodologies | 3-7 |
| 303 | Risk Assessment Process | 3-7 |
| 304 | Protective Measures to Prevent Misuse and Abuse | 3-10 |
| 305 | Certification Process | 3-10 |
| | a. New or Modified Applications | 3-11 |
| | b. Recertifications | 3-12 |
| 306 | Procedures for Screening Non-Federal Personnel | 3-13 |
| | a. Scope and Applicability | 3-13 |
| | b. Objective | 3-13 |
| | c. Screening Procedure | 3-13 |
| 307 | Controlling Access By Foreign Nationals | 3-14 |
| | a. Introduction | 3-14 |
| | b. Purpose | 3-14 |
| | c. Categories | 3-14 |
| | d. Sponsors | 3-14 |
| | e. Submission/Approval of Requests | 3-16 |
| | f. Exceptions | 3-16 |
| 308 | Contingency and Disaster Recovery Planning | 3-16 |
| | a. Definitions | 3-16 |
| | b. Plan Content | 3-18 |
| 309 | Computer Security Incident Response (CSIR) Capability | 3-19 |
| | a. Responsibilities | 3-19 |
| | b. Objectives | 3-19 |
| | c. Procedure Elements | 3-19 |
| | d. Non-duty Hours Considerations | 3-21 |
| 310 | Computer Security Awareness and Training (CSAT) | 3-21 |
| | a. Continuous CSAT | 3-21 |
| | b. Multifaceted Approach | 3-23 |
| 311 | Procurement of Products and Services | 3-24 |
| | a. Introduction | 3-24 |

| Paragraph | | Page |
|---|---|---|
| | b. NASA Contracting Environment | 3-25 |
| | c. Project Manager Responsibilities | 3-25 |
| | d. Sponsoring Organization Responsibilities | 3-25 |
| | e. Contracting Officer Responsibilities | 3-25 |
| | f. Evaluating Security Capabilities | 3-26 |
| | g. Contract Administration | 3-26 |
| | h. Requirements for Contractor-Operated DPI's | 3-26 |
| | CHAPTER 4. AUTOMATED INFORMATION CATEGORIES AND SENSITIVITY/CRITICALITY LEVELS | |
| 400 | Introduction | 4-1 |
| | a. Information Categories | 4-1 |
| | b. Sensitivity/Criticality Levels | 4-3 |
| 401 | Information Categories | 4-4 |
| 402 | Sensitivity/Criticality Levels | 4-8 |
| | a. Introduction | 4-8 |
| | b. Automated Information and Applications | 4-8 |
| | c. Computer Systems | 4-8 |
| 403 | Protection Measure Baseline Considerations | 4-10 |
| | a. Sensitivity/Criticality Level 0 | 4-10 |
| | b. Sensitivity/Criticality Level 1 | 4-11 |
| | c. Sensitivity/Criticality Level 2 | 4-11 |
| | d. Sensitivity/Criticality Level 3 | 4-12 |
| | CHAPTER 5. COMPUTER SECURITY PLANNING | |
| 500 | Introduction | 5-1 |
| 501 | Headquarters Computer Security Planning | 5-1 |
| | a. NASA Automated Information Security Program Plan | 5-1 |
| | b. Program Office Computer Security Plan (PO-CSP) | 5-2 |
| 502 | Center Computer Security Planning | 5-3 |
| | a. Center Computer Security Plan (CCSP) | 5-3 |
| | b. Content and Format | 5-4 |
| 503 | DPI Computer Security Planning | 5-6 |
| | a. Purpose | 5-6 |
| | b. Content | 5-6 |

| Paragraph | | Page |
|---|---|---|
| 504 | DPI Contingency and Disaster Recovery Plans | 5-8 |
| 505 | External Requests for Reports on Planning Activity | 5-8 |
| | CHAPTER 6. SPECIAL CONSIDERATIONS FOR MICROCOMPUTERS | |
| 600 | Introduction | 6-1 |
| | a. Security Principles | 6-1 |
| | b. Security Implications | 6-1 |
| 601 | Special Protective Measures for Microcomputers | 6-1 |
| | a. Technical Protective Measures | 6-1 |
| | b. Administrative Protective Measures | 6-2 |
| | c. Physical Protective Measures | 6-2 |
| | d. Personnel Protective Measures | 6-2 |
| | APPENDICES | |
| APPENDIX A. | REFERENCES | A-1 |
| APPENDIX B. | ABBREVIATIONS | B-1 |
| APPENDIX C. | DEFINITIONS | C-1 |
| APPENDIX D. | LIST OF EXHIBITS | D-1 |
| APPENDIX E. | CLASSIFIED SYSTEM SECURITY PLAN | E-1 |

# CHAPTER 1. PROGRAM OVERVIEW

## 100 INTRODUCTION

a. Management Issue. Computer security is an increasingly important issue for all NASA managers. Modern technology and the demands of space research have made NASA more and more dependent on computers to store and process vast amounts of information that support sensitive and mission-critical functions. NASA's computer and information assets have such great value that they must be managed to the same extent as the more traditional organizational assets (i.e., people, money, equipment, natural resources, and time).

b. Value of Information and Computing Resources. The value of NASA's information and computing resources and the importance of NASA missions create a need for these resources to be adequately protected to assure availability, integrity, and confidentiality, as appropriate. The appropriate protection of automated information must be motivated and supported by the managers who own or use that information.

c. Life-Cycle Phases. Some automated systems are acquired "off the shelf" and can be used immediately. Others must be specially designed, developed, and implemented over months or years. Once an automated system is fully operational, the options available to provide computer security are somewhat limited. However, if security is designed into an automated system, the safeguard options are vastly increased and the safeguard costs over the life of the system are substantially reduced. This is true for computer hardware, system software, and application software. Therefore, it is important for NASA managers to ensure that security is appropriately addressed in all phases of the life cycle for automated systems, especially in the early planning stages.

d. History. In the past, NASA computer security guidance was provided through the following:

(1) NASA Handbook (NHB) 2410.1, "Information Processing Resources Management," April 1985.

(2) Assorted NASA policy letters, such as:

(a) "Interim Standard for Identification of NASA Sensitive Automated Information and Applications," NASA Headquarters (HQ) Code NT letter, November 1987.

(b) "Responding to and Reporting Automated Information Security Incidents," NASA HQ Code NT letter, January 1988.

(3) Assorted NASA guidelines, such as:

(a) "Guidelines for Certification of Existing Sensitive Systems," July 1982.

(b) "Guidelines for Development of NASA Computer Security Training Programs," May 1983.

(c) "Guidelines for Developing NASA ADP Security Risk Management Plans," August 1983.

(d) "Guidelines for Developing NASA ADP Security Risk Reduction Decision Studies," January 1984.

(e) "NASA ADP Risk Analysis Guidelines," July 1984.

(f) "NASA Guidelines for Assuring the Adequacy and Appropriateness of Security Safeguards in Sensitive Applications," September 1984.

(g) "NASA Guidelines for Meeting DOD Accreditation Requirements for Processing Classified Data," March 1985.

(h) "Guidelines for Contingency Planning," November 1982.

(i) "Guidelines for Selection of Backup Strategies," November 1982.

e. References. Appendix A lists the references used in this Handbook, which expands on NMI 2410.7, "Assuring the Security and Integrity of NASA Automated Information Resources," and replaces the following:

(1) NHB 2410.1, Chapter 3.

(2) All prior computer security policy letters.

(3) All of the documents listed in subparagraph d(3).

f. Terminology. Appendix B is a list of abbreviations. Appendix C provides definitions for most of the terms used in this Handbook. Given the number of terms unique to the computer and/or security disciplines, readers should familiarize themselves with the definitions in Appendix C before going on to Chapter 2.

## 101 PURPOSE

The purpose of this Handbook is to present more specific guidance on the general computer security management philosophies, policies, and requirements outlined in NMI 2410.7. This Handbook is intended to be used by the Center Computer Security Managers (CCSM's) and HQ Program Office Computer Security Managers (PO-CSM's). This Handbook is not intended to be site specific. Centers are encouraged to supplement this Handbook with procedures, duties, and titles in order to tailor guidance to their unique environments.

## 102 ORGANIZATIONAL SCOPE

a. The provisions of this Handbook apply to all NASA organizations and support contractor organizations as provided by law and/or contract and as implemented by the appropriate contracting officer. Generally excluded are contractor or research facility computing and information resources not under direct NASA management cognizance or that are merely incidental to a contract (e.g., a contractor's payroll and personnel system). The managing organization (i.e., NASA center or NASA HQ Program Office) may, through the appropriate contracting officer, elect to include any information and computing resources excluded by this Handbook.

b. Within reason, the provisions of this Handbook should be applied in university environments (where NASA is supported through formal agreements such as grants, cooperative agreements, contracts, and purchase orders). NASA managers/sponsors of such activities should take a reasonable approach that will not impose unnecessary constraints on the open university environment. The extent of compliance with this Handbook in university environments needs to be evaluated on a case-by-case basis and may range from minimal compliance (i.e., for one-time research activities in which there is no clear indication that NASA is the information owner) to more stringent compliance (i.e., for universities processing NASA-owned information on a long-term

basis). A risk assessment should be conducted to identify acceptable risk exposures and determine how unacceptable risk exposures can reasonably be reduced to more acceptable levels.

## 103 SYSTEMS COVERED

This Handbook covers the protection of all NASA computer systems including the information they store and process. It also provides for the continuity of operations of computer systems and applications.

## 104 EXCEPTIONS

In certain situations, other protective measures may already be in place to meet the general requirements contained in this Handbook. Exceptions from implementing the specifics of this Handbook may be granted by the managing organization overseeing the data processing installation's (DPI) activities. Delegation of this exception authority shall be no lower than the CCSM. PO-CSM's have exception authority for systems under their purview.

## 105 NASA COMPUTER SYSTEMS ENVIRONMENT

NASA represents one of the larger, more complex, and diverse computing environments in the Federal Government. NASA has an annual information technology resource budget exceeding $1 billion that supports nine NASA centers and the Jet Propulsion Laboratory (JPL). It is recognized that while JPL is viewed as a NASA center, it is a facility performing research and development for NASA under contract to California Institute of Technology (Caltech) and thus NASA policy is applicable to JPL to the extent provided for in the NASA/Caltech contract. These centers manage computer resources on a decentralized basis at a large number of DPI's, many of which are operated under contract. The computer system configurations range from the largest mainframe and supercomputers to minicomputers, microcomputers, and intelligent/engineering work stations. Computing operations support earth and space mission functions for a full array of processing environments ranging from administrative computing in office settings to scientific and engineering computing in academic, research center, production plant, and space vehicle environments. Providing appropriate protection in such diverse environments involves a continuing management process of balancing user needs for unrestricted access to information with the sometimes conflicting requirements to control access and preserve integrity.

## 106 IMPORTANCE OF AN EFFECTIVE COMPUTER SECURITY PROGRAM

a. Public Image. NASA has high public visibility due to the nature of its operations. Human safety during manned space flight and the success of research and military missions in space are highly dependent on the reliability of supporting computer resources and the integrity of automated information. Public and Congressional confidence in the Space Program are directly keyed to the clarity of NASA's commitment to excellence in all areas.

b. Increasing Incidents. In recent years all Federal agencies have experienced an increase in international electronic intrusions and electronic worm/virus penetrations. These problems are expected to become more technically complex and more widespread with advancements in computer and telecommunication technologies. Therefore, it has become increasingly important to develop a Computer Security Incident Response (CSIR) capability to minimize the effects of such incidents. See paragraph 309 for details of such a response capability.

c. Management Priority. The importance to senior NASA management of an effective computer security program was indicated by the NASA Administrator in a policy letter dated July 8, 1988, to all NASA employees. The letter expressed the Administrator's personal expectations for "full support ... cooperation ... and an aggressive program ...."

## 107 NASA AUTOMATED INFORMATION SECURITY PROGRAM BACKGROUND

a. Initial Policy. In 1979 NASA formally implemented its computer security program by defining and promulgating agencywide policies regarding the security and integrity of agency computing facilities. The main focus was on maintaining continuity of operations and minimizing the potential for improper use of computing facilities. These policies were issued in accordance with the Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, July 27, 1978, "Security of Federal Automated Information Systems." This memorandum required each Federal agency to establish a computer security program.

b. Initial Handbook. NASA's basic computer security policy was augmented in 1980 with the publication of extensive guidelines for implementing computer security requirements within the agency. These guidelines were published in NHB 2410.1, "Information Processing Resources Management." NHB 2410.1 was updated in 1982 and again in 1985. NASA operated under its basic policy (circa 1979) until 1988, when it published NMI 2410.7, "Assuring the Security and Integrity of NASA Automated Information Resources." NASA then began restructuring its computer security program to bring the agency into compliance

with the Ccmputer Security Act of 1987 and technological advances in computing and telecommunication systems.

c. Summary of Other Milestones. The agency has had an established computer security program since 1979; a full-time automated Information Security Program Manager since 1985; computer security awareness and training (CSAT) since 1983; and management evaluations of agency computer security activities since 1979.

108 ORIGIN OF NATIONAL POLICY

a. National Organizations. As presented in Exhibit 1-1, the NASA Automated Information Security Program is based on public laws promulgated by Congress. The following organizations then issued national policies, standards, and guidelines:

(1) The Department of Commerce (DOC).

(2) The National Institute for Standards and Technology (NIST).

(3) The Office of Management and Budget (OMB).

(4) The Office of Personnel Management (OPM).

(5) The National Security Agency (NSA).

(6) The Department of Defense (DOD).

(7) The General Services Administration (GSA).

(8) Various Presidential committees on computer and telecommunications systems security.

b. National Documents. National policy and guidance documents include:

(1) Computer Security Act of 1987 (PL 100-235).

(2) Executive Order 12356.

(3) OMB Circular A-130.

(4) NIST Federal Information Processing Standards (FIPS) Publications.

(5) DOD guidance on protecting classified information.

(6) NSA guidance on trusted computer systems.

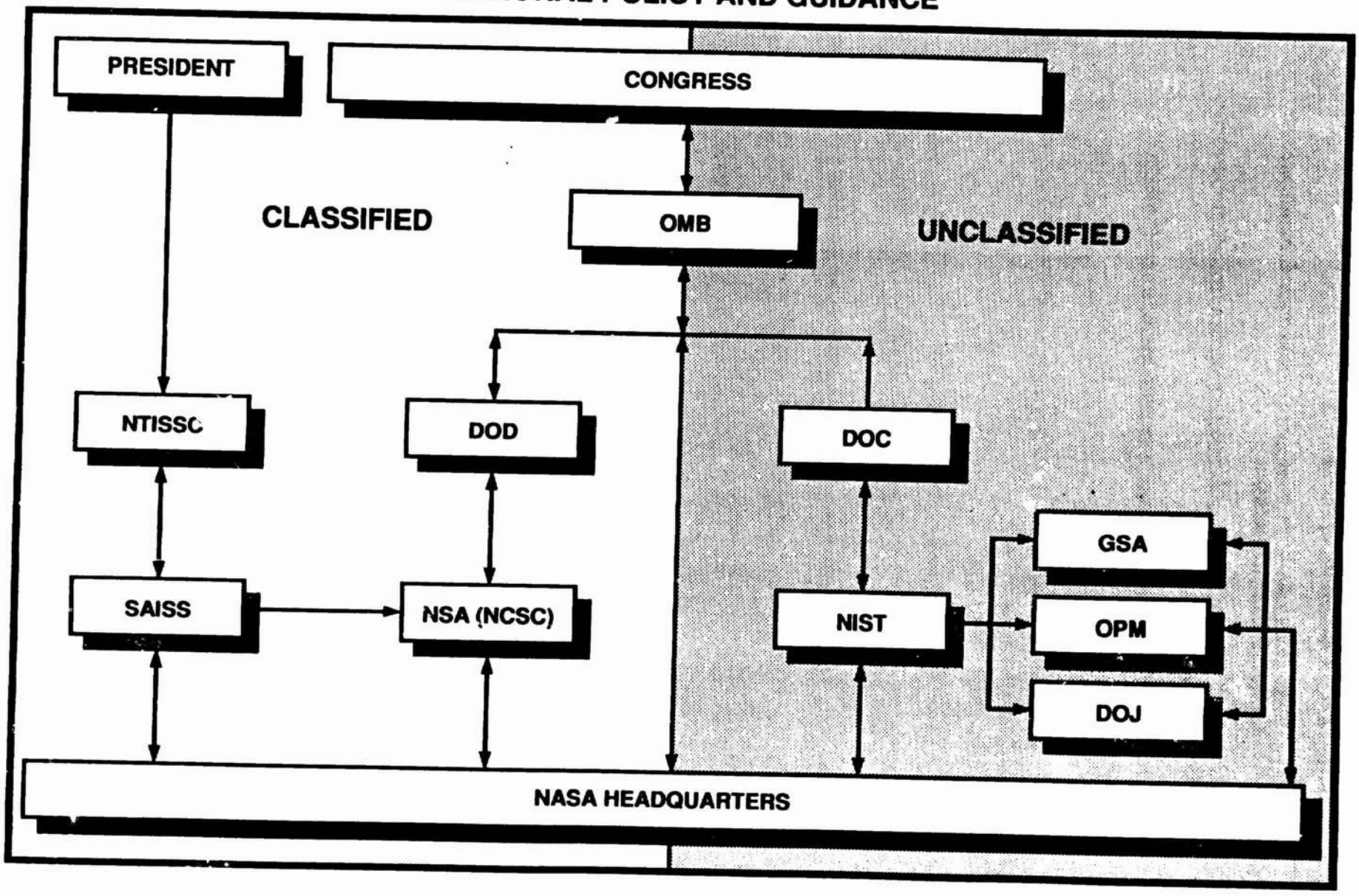
(7) OPM Personnel Letter 732.

(8) GSA Federal Information Resource Management Regulation (FIRMR).

(9) GSA Federal Information Processing Management Regulation.

(10) GSA Federal Acquisition Regulation (FAR).

## EXHIBIT 1-1
## NATIONAL POLICY AND GUIDANCE



# CHAPTER 2. PROGRAM ORGANIZATION AND MANAGEMENT

## 200 INTRODUCTION

**This Chapter covers the NASA Automated Information Security Program goal, objectives, organizational structure and management.**

## 201 MANAGEMENT PHILOSOPHIES

a. Integration. The NASA Automated Information Security Program is designed to provide appropriate, cost-effective protection for sensitive, classified, mission critical, life support, and high-dollar-value information and computing resources. In this regard, NASA has an extensive computer security program that is highly integrated into its management functions through points-of-contact, intra-agency working groups, councils, and committees. These management and coordinating bodies range from a senior management Information Resources Management (IRM) Council to CCSM's, local Data Processing Installation Computer Security Officials (DPI-CSO's), and Computer Security Coordinators (CSC's) at the computer system level.

b. Decentralization. Due to NASA's highly decentralized approach to managing a large number of diverse computer environments nationwide, a decentralized approach for managing automated information security has been taken. NASA HQ interprets national policy and guidance and issues general policy and guidance appropriate for the NASA computing environment. Each center is responsible for establishing and sustaining a computer security program that assures that each DPI under its cognizance complies with computer security requirements that are consistent with the DPI's unique computing environment. Specific protective decisions (e.g., cost-effective approaches, benefits to be derived) are made by management at the center and DPI levels based on risk assessment activities. Functional security requirements and technical security specifications are to be integrated into appropriate system life-cycle phases and appropriate security-related responsibilities included in job descriptions and performance evaluation criteria. Compliance is assured through multiple levels of top-down management and compliance review activities.

c. Perfection. A state of absolute protection is not practical nor desirable in most cases. Numerous reasons include the following:

(1) Absolute protection would make the agency's systems virtually unusable by the research community for which the agency's mandate, under the Space Act of 1958, is to provide the most useful information to the widest possible audience.

(2) Some vulnerabilities may not be known, as in the case where vendor-supplied operating systems contain security flaws.

(3) Computer and network technology is constantly advancing at a rapid pace. While these advances create new opportunities for our scientists and engineers, they also offer new opportunities for those who wish to do mischief.

(4) Protection must be applied in a cost-effective manner in order to meet agency responsibilities in its expenditures of public funds.

## 202 NASA AUTOMATED INFORMATION SECURITY PROGRAM GOAL AND OBJECTIVES

a. Goal. The goal of the NASA Automated Information Security Program is to provide cost-effective protection that assures the integrity, availability, and confidentiality of NASA automated information resources. Thus, the main focus in scientific and engineering environments is to provide appropriate cost-effective protection and management emphasis that assures the appropriate levels of information integrity and computing resource availability without unnecessarily impacting innovative productivity or the advancement of technology. In these environments and in the administrative environments, where the sensitive or classified nature of information calls for mandatory or discretionary protection from unauthorized disclosure, additional consideration must be given for providing cost-effective protection that assures information confidentiality.

b. Objectives. The objectives of the NASA Automated Information Security Program are to:

(1) Protect against deliberate or accidental corruption of NASA automated information.

(2) Protect against deliberate or accidental actions that cause NASA automated information resources to be unavailable to users when needed.

(3) Ensure that there is no deliberate or accidental disclosure of NASA sensitive or classified automated information.

## 203 PROGRAM ELEMENTS

a. Basic Elements. The basic elements of the NASA Automated Information Security Program are illustrated in Exhibit 2-1. They are to be employed in appropriate combinations to adequately protect sensitive, critical, valuable, and important NASA information and computing assets at acceptable levels of risk. The NASA Automated Information Security Program covers both classified and unclassified assets.

(1) Computer Security Policy/Guidance. Computer security policies and guides are needed to define the overall framework (including lines of authority, main points-of-contact, range of responsibilities, requirements, procedures, and management processes) for implementing and sustaining an efficient and cost-effective NASA Automated Information Security Program.

(2) Computer Security Planning. Computer security planning must provide a consistent and specific approach for determining short- and long-range management objectives, developing security enhancement proposals, mapping proposals to budget requests, and assuring the implementation of appropriate cost-effective protective measures.

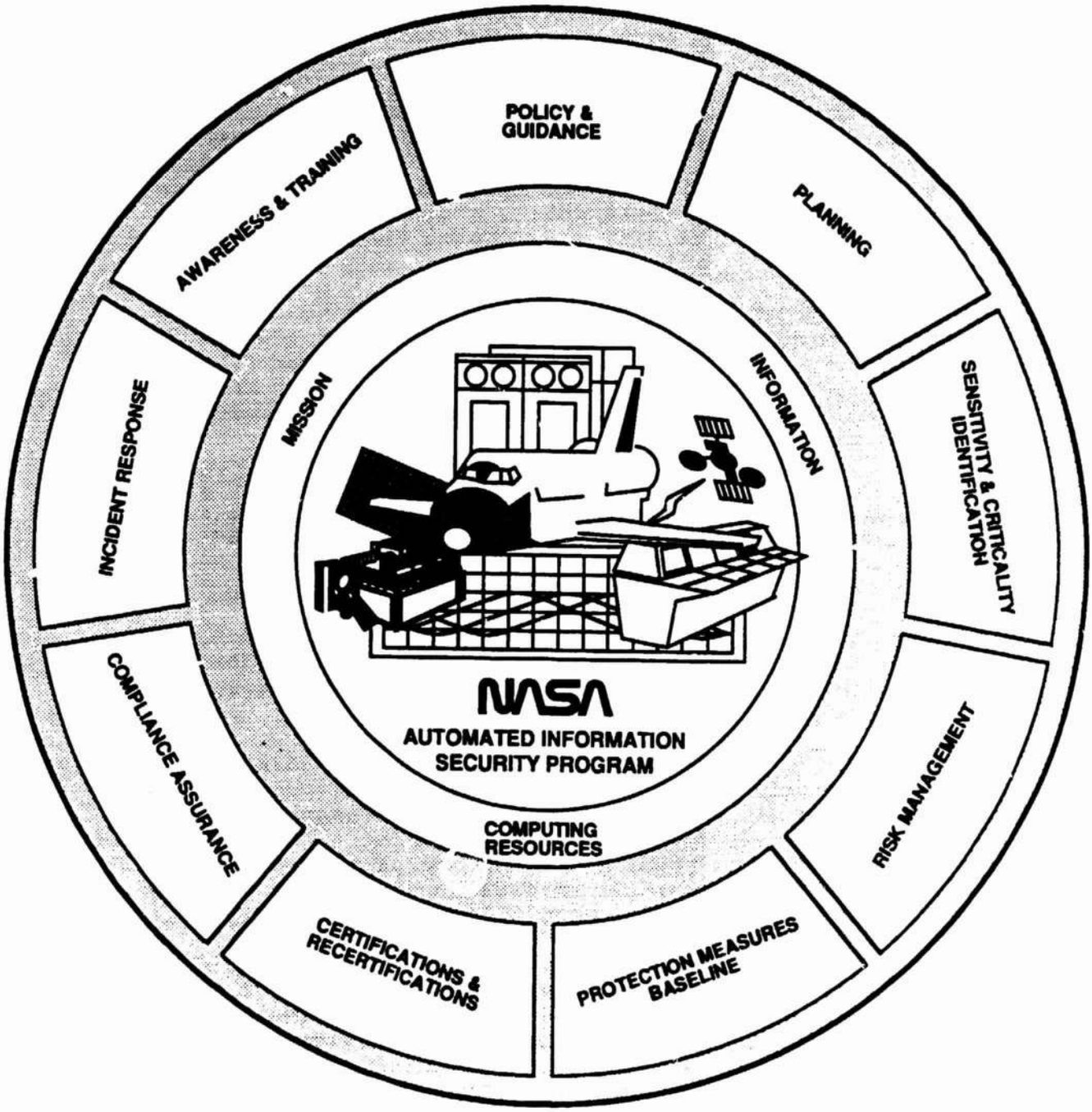
(3) Sensitivity and Criticality Identification. The information and computing resources used to support NASA missions have various levels of sensitivity and criticality. These levels need to be determined, since they are critical to deciding which protective measures are most appropriate.

(4) Risk Management. NASA managers need to continually identify and analyze potential threats to NASA's computing environments and reduce risk exposures to acceptable levels. This process is called risk management.

(5) Protective Measure Baseline. There are numerous combinations of technical, physical, administrative, and personnel protective measures available to NASA managers. A baseline of these protective measures needs to be defined/suggested to facilitate development of acceptable levels of protection for computing and information resources managed by NASA or operated/processed in support of NASA missions.

(6) Certifications/Recertifications. Certifications and recertifications of automated applications document that current risk levels are acceptable. They also document the accountability for the acceptance of residual risks and complete the evaluation process for protective measures (controls and checks) programmed into automated applications.

# EXHIBIT 2-1
# NASA AUTOMATED INFORMATION SECURITY PROGRAM LOGO



(7) **Multilevel Compliance Assurance Mechanism.** Management and compliance reviews should be periodically conducted to sustain optimal security levels at all centers and DPI's.

(8) Incident Response. It is necessary to develop specific and appropriate responses to the various security incidents that may occur. It is also necessary to provide feedback information to senior management on significant incident situations. This information also supports the tracking of agencywide trends.

(9) Continuous CSAT. Continuous CSAT is necessary to elevate and sustain management and personnel awareness and provide specific guidance to personnel who design, implement, use, or maintain computer systems.

b. Sustaining Program Effectiveness. After policies and procedures have been established and initial security management tasks have been accomplished at the centers and DPI's, the ongoing aspects of risk assessment, recertification, computer security awareness and training, and compliance review activities should continually refresh local automated information security programs and keep them alive. The ongoing aspects of significant incident reporting and annual submission of automated information security program plans should provide managers at the center and HQ levels with sufficient information to continually reassess current program status and determine future management direction.

## 204 NASA COMPUTER SECURITY POLICY

It is NASA policy that:

a. Technical,
b. Personnel,
c. Administrative,
d. Environmental, and
e. Access

protective measures be used, alone or in combination, to cost-effectively provide an appropriate level of protection for NASA automation assets, and especially for automated information. The rigor of controls should be commensurate with the sensitivity level of the information resources to be protected. Selection of protective measures for a specific computing environment should be based on an assessment of risks and the existence of reasonable ratios between the costs/benefits of proposed protective measures and the sensitivity, criticality, and/or value of the assets requiring protection. Appropriate emphasis should be placed on:

f. Automated information,
g. Computer hardware, and
h. Computer software

to assure that they are appropriately protected from threats that include unauthorized:

i. Access,
j. Alteration,
k. Destruction,
l. Removal (e.g., theft),
m. Disclosure,
n. Use/abuse, and
o. Delays

as a result of improper actions or adverse events.

## 205 HEADQUARTERS ROLE AND RESPONSIBILITIES

a. Overview. There are many organizations that have roles and responsibilities related to implementing and managing the NASA Automated Information Security Program, although the Head of each Federal agency has ultimate responsibility.

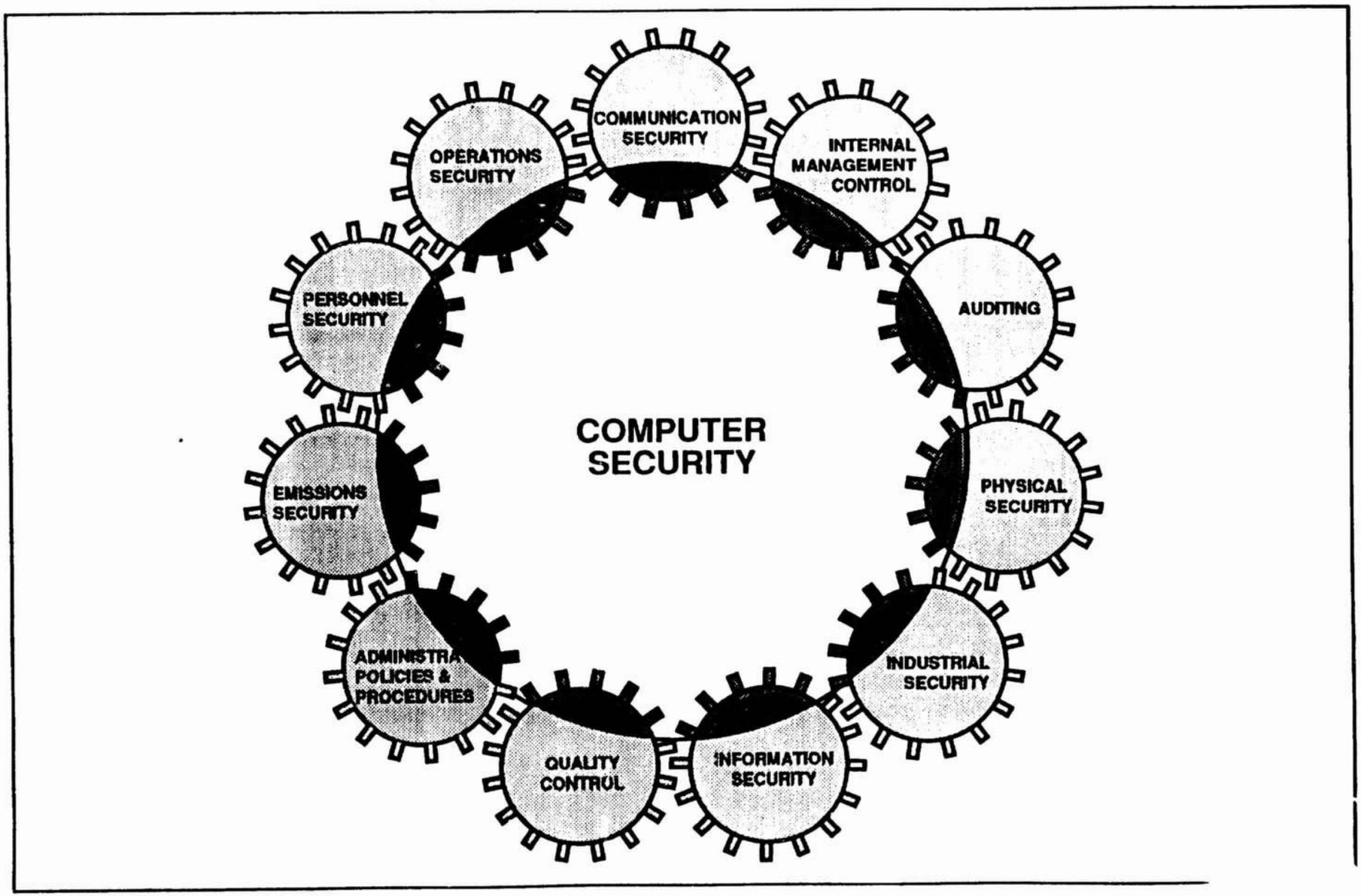
b. Multidisciplinary Coordination

(1) Management Disciplines. All traditional management disciplines and functions must be employed in a coordinated fashion to effectively manage security. The reason for this multidisciplinary situation is that, over the years, NASA has become more electronically-based and dependent on automation technologies to support all aspects of its operations and missions.

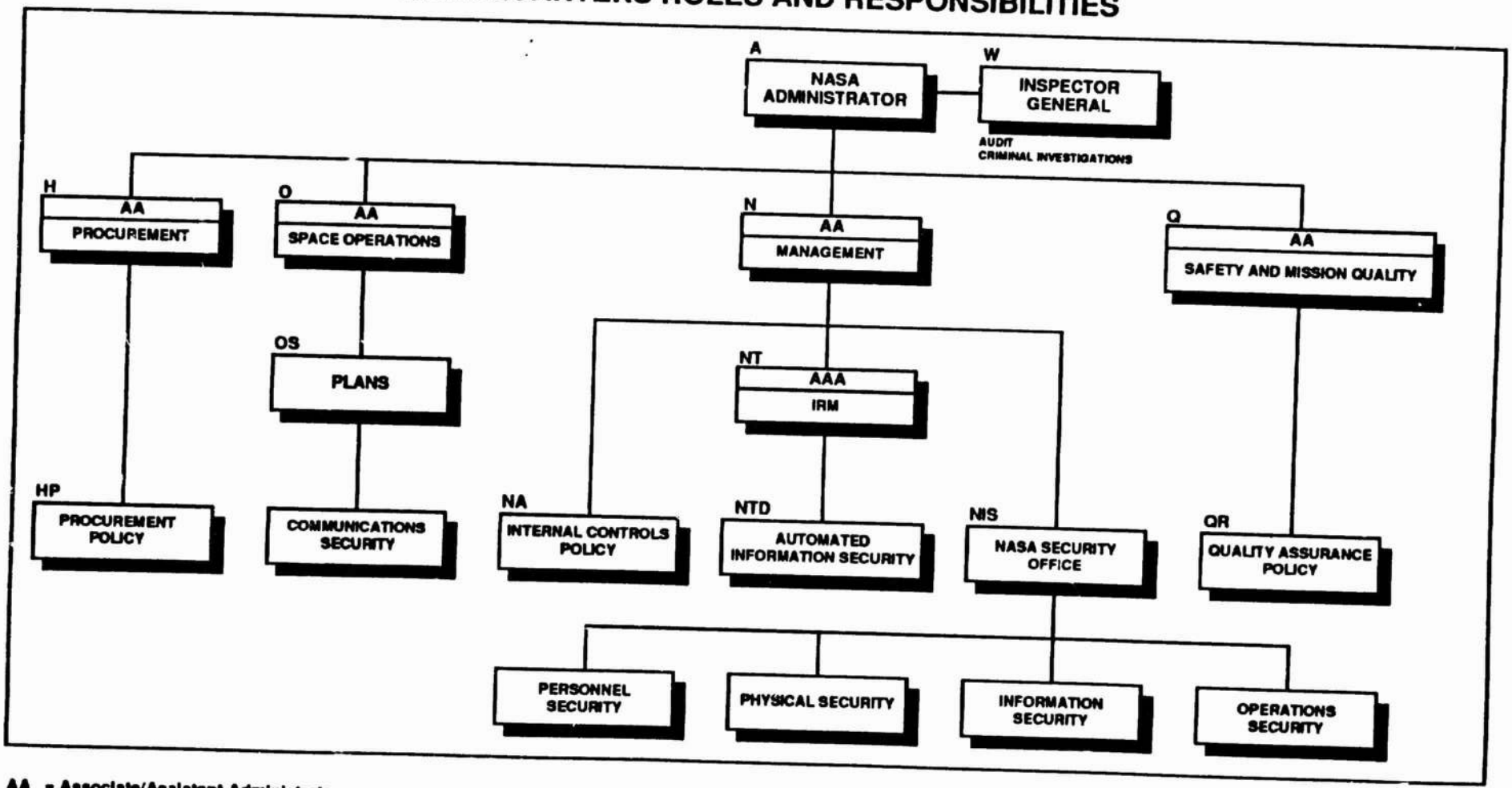
(2) Security Disciplines. As shown in Exhibit 2-2, there are many security-related disciplines, each with its own set of policies and procedures. Each security discipline is almost always an entirely separate career field throughout the Federal Government. Only when all such disciplines are working together, in a highly coordinated fashion, can the entire security process function properly and efficiently. Thus, it is important for computer security managers at all levels to regularly coordinate with other security-related disciplines.

c. NASA Automated Information Security Program Manager. As shown in Exhibit 2-3, NASA primary authority for managing an agencywide computer security program has been delegated through the Assistant Administrator for Management to the Assistant Associate Administrator for IRM. In addition to the general requirements of NMI 2410.7:

## EXHIBIT 2-2
## COMPUTER SECURITY'S RELATIONSHIPS WITH OTHER SECURITY DISCIPLINES



# EXHIBIT 2-3
# HEADQUARTERS ROLES AND RESPONSIBILITIES




AA = Associate/Assistant Administrator
AAA = Assistant Associate Administrator

(1) The Assistant Associate Administrator for IRM shall:

(a) Designate a management official knowledgeable in both computing and computer security management principles and practices to be the NASA Automated Information Security Program Manager; and

(b) Apprise Center Directors, through appropriate Program Associate Administrators, of program management reviews conducted in response to the requirements of NMI 2410.7 and this Handbook and make recommendation for improvements, as appropriate.

(2) The NASA Automated Information Security Program Manager shall:

(a) Serve as an agency focal point of coordination among NASA senior management, HQ Program Offices, centers, and external organizations on automated information security matters.

(b) Develop and coordinate the implementation of agency plans, policies, procedures, and guidelines related to the requirements of NMI 2410.7 and this Handbook.

(c) Conduct program management reviews of centers to assess the sustained effectiveness of center management oversight processes that have been implemented at DPI's under center management cognizance and make recommendations to the Assistant Associate Administrator for IRM, through the Director, IRM Policy Division, for improvement, as appropriate.

(d) Coordinate the review and dissemination of information identifying emerging trends to keep NASA management informed.

d. Headquarters Program Offices. In addition to the general requirements of NMI 2410.7, Program Associate Administrators shall:

(1) Promulgate Program Office specific policies, procedures, and guidelines related to the general requirements of NMI 2410.7 and this Handbook, as deemed appropriate.

(2) Designate a management official knowledgeable in both computing and computer security methods and practices to be the PO-CSM. The PO-CSM should serve as a focal point to coordinate agencywide activities required in NMI 2410.7 and this Handbook between the HQ Automated Information Security Program Manager and cognizant Program Office organizations. In cases

where multiple organizational levels or program area applications exist, Assistant PO-CSM's and/or CSC's may be designated to accomplish specific computer security responsibilities.

(3) Implement and coordinate an appropriate management oversight process that ensures awareness and compliance with applicable portions of NMI 2410.7 and this Handbook in cognizant organizations.

(4) Assure that all NASA and appropriate NASA contractor computing and telecommunications resources processing NASA information are identified and included under the management of a DPI.

(5) Assure that, through the contracting officer, all appropriate contractors are required to comply with applicable provisions of NMI 2410.7 and this Handbook.

(6) Review and concur on exceptions from implementing specific requirements of this Handbook.

e. Other Headquarters Offices. Other HQ offices that play an integral role include the:

(1) Inspector General, which has independent audit and criminal investigation responsibilities.

(2) NASA Security Office, which has traditional security responsibilities in the areas of personnel security, physical security, and national (including defense-related) security documents and operations control.

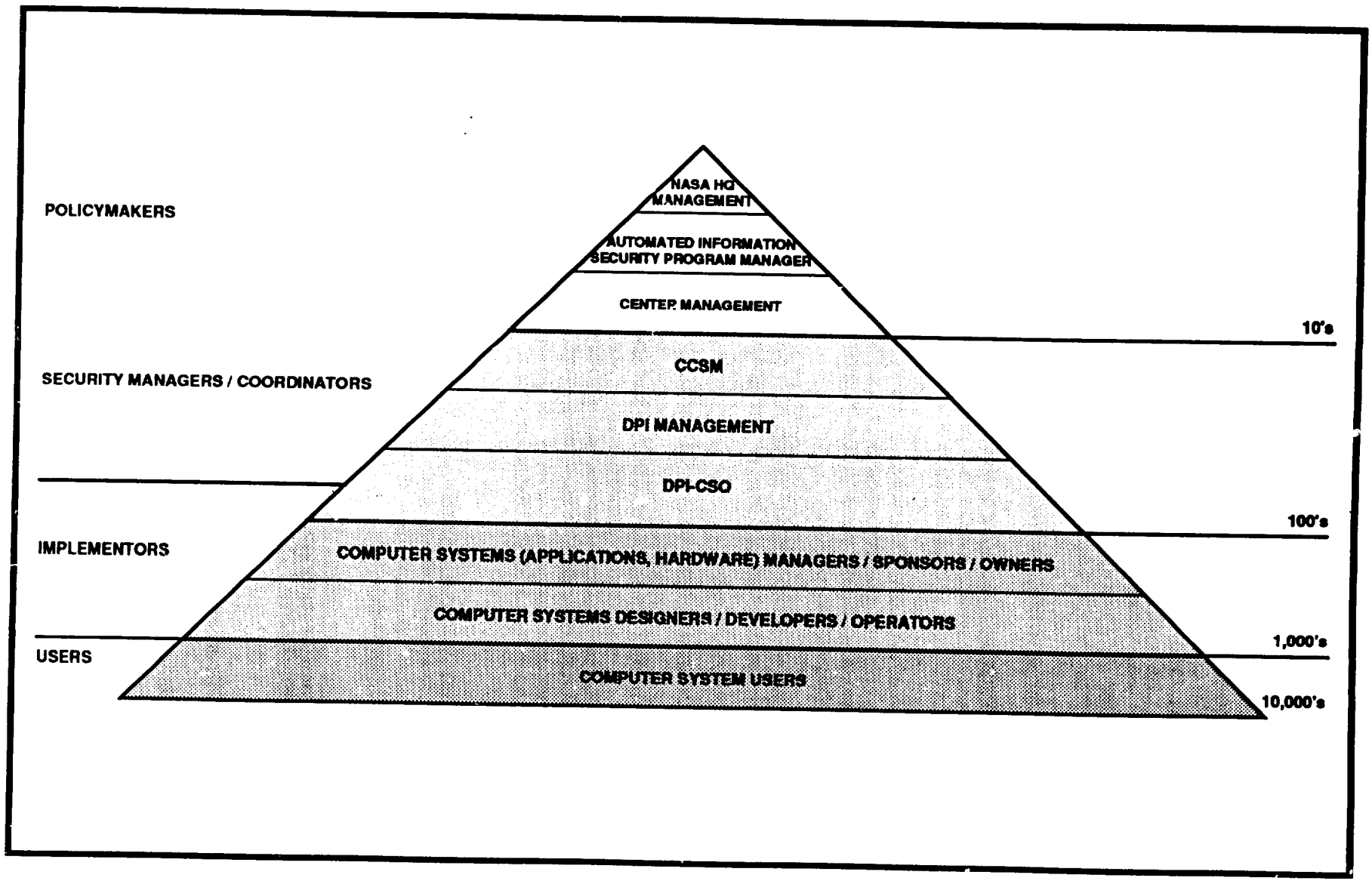
(3) Office of Space Operations, which has agencywide responsibilities for telecommunications security.

(4) Office of Procurement, which has responsibilities for ensuring that appropriate functional security requirements are included in acquisitions for automated information products and services.

(5) Management Operations Office, which has responsibilities for the NASA Internal Controls Program.

(6) Office of Safety, Reliability, Maintainability, and Quality Assurance, which has responsibilities related to automated information resources supporting manned space flight.

## EXHIBIT 2-4
## WHO IS RESPONSIBLE FOR AUTOMATED INFORMATION SECURITY?



## 206 INDIVIDUAL RESPONSIBILITIES FOR COMPUTER SECURITY

As illustrated in Exhibit 2-4, the situation discussed in paragraph 205 dictates that virtually everyone in the organization who manages, designs, programs, operates, or uses NASA automated information resources has personal job-related responsibilities that contribute toward meeting the goal and objectives of the NASA Automated Information Security Program. The practice of effective computer security management principles normally becomes an integral function of good business/ professional practice when it can be demonstrated that positive benefits can be derived. For example:

a. Appropriately restricting unauthorized access can greatly contribute to ensuring information/system integrity and availability.

b. Systems that are well planned and passed through a quality assurance/certification process are normally more efficient and have fewer maintenance problems in operational use.

c. Technology that is used in a controlled environment can be expected to have greater reliability.

## 207 PROGRAM ORGANIZATIONAL STRUCTURE

a. In order to effectively manage the day-to-day aspects of a computer security program, in a large and diverse organization like NASA, a network of designated managers must be established at all levels throughout the organization. Exhibit 2-5 illustrates the relationship between NASA-designated computer security managers and officials at the HQ, center, and DPI levels.

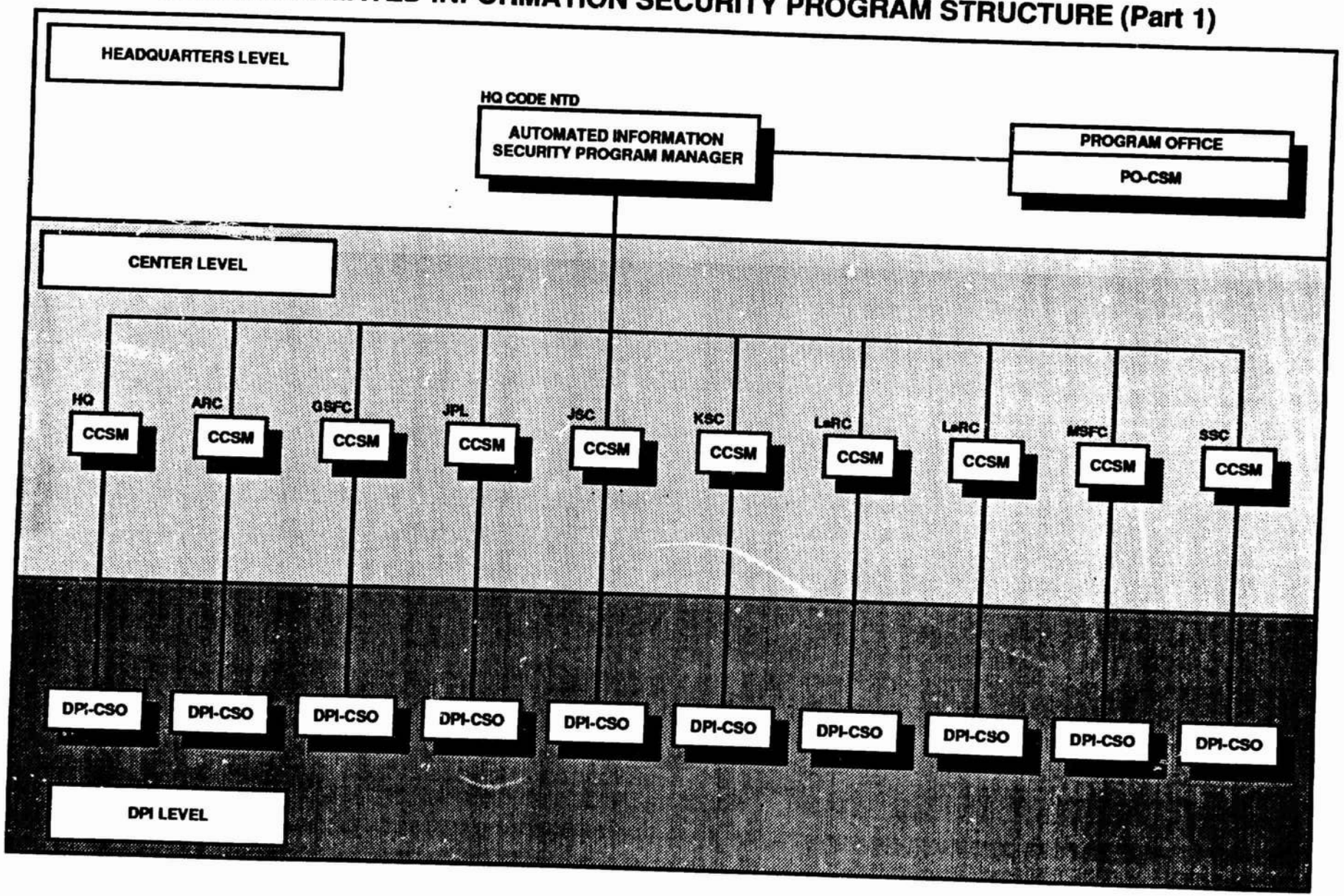
b. Headquarters Level. The NASA Automated Information Security Program Manager has a direct working relationship and communications link with HQ PO-CSM's and CCSM's to focus on resolving NASA issues.

c. Center Level. Each CCSM has a direct working relationship and communication link with DPA-CSO's to focus on resolving center-level issues.

## 208 MANAGEMENT REVIEW AND COMPLIANCE ASSURANCE PROCESS

Since computer security compliance levels have an inherent tendency to degrade with time, management reviews are necessary

# NASA AUTOMATED INFORMATION SECURITY PROGRAM STRUCTURE (Part 1)



to retain a high level of compliance. Therefore, the NASA Automated Information Security Program will require periodic management reviews at all levels.

a. Headquarters Reviews. NASA HQ will conduct periodic management reviews of centers to evaluate their management and coordination of programs at DPI's under their cognizance.

b. Center Reviews. Centers will conduct periodic compliance reviews at DPI's under their cognizance at least every 1 to 3 years. Review activities should be focused in the following four areas:

(1) Tracking Systems and Random Checks. Tracking systems are needed to monitor recommendations from review activities (e.g., compliance reviews, recertifications, risk assessments). Random checks and tests ensure actual implementations of appropriate procedures and that protective measures do, in fact, reduce identified risk exposures to acceptable levels.

(2) Security Incidents. Reported security incidents should be tracked to determine trends, to identify general problem areas and security needs, and to ensure implementation of appropriate procedures and protective measures. The result should be fewer incidents.

(3) Contingency Planning. Contingency and disaster recovery plans provide overall protection when other safeguarding features may have failed. Such plans should be in place and periodically tested, at a minimum, for the most sensitive and critical systems.

(4) CSAT. Managers should ensure that continuous CSAT is conducted at DPI's, as appropriate.

c. DPI Reviews. Each DPI will conduct ongoing self-assessment review activities to include CSAT, risk assessments, and recertification reviews of applications supporting sensitive or mission-critical functions to sustain optimal levels of security.

# CHAPTER 3. CENTER AND DPI REQUIREMENTS

## 300 CENTER REQUIREMENTS

a. Designation of Authorities. In addition to the general requirements of NMI 2410.7, Center Directors shall:

(1) Promulgate specific center policies, procedures, and guidelines related to the general requirements of NMI 2410.7 and this Handbook, as deemed appropriate; and

(2) Designate, in writing, a management official knowledgeable in both computing and computer security methods and practices to be the CCSM.

b. CCSM Responsibilities. The CCSM shall serve as a focal point to manage a program that is responsive to the Center Director and coordinate activities required by NMI 2410.7 and this Handbook between the HQ Automated Information Security Program Manager and cognizant DPI's. In cases where multiple DPI's exist, Assistant CCSM's may be designated to accomplish specific center computer security responsibilities. The CCSM responsibilities include:

(1) Implementing and coordinating an appropriate management oversight process that ensures awareness and compliance with the Center Computer Security Program.

(2) Assuring that each NASA and appropriate NASA contractor DPI under his/her cognizance develops, implements, and sustains an effective computer security program that ensures awareness and compliance at the DPI level.

(3) Scheduling and conducting periodic compliance reviews at cognizant DPI's to assess the adequacy of security plans, the sustained effectiveness of its computer security procedures and program, and to make recommendations for improvement, as appropriate. Compliance reviews should be conducted every 1 to 3 years based on the reviewing management's judgement. Factors to be considered in making this decision include the reviewing management's perception of the sensitivity, criticality, and/or value of the computing and information assets to be protected at each DPI.

(4) Assuring that procedures are implemented for identifying computer security incidents that occur at DPI's under his/her cognizance. These procedures shall ensure that

significant computer security incidents are reported to the HQ Automated Information Security Program Manager immediately following detection and that significant incident information received from HQ is disseminated to cognizant DPI's. (See paragraph 309 for a description of this procedure.)

(5) Assuring that, through the contracting officer, all appropriate contractors comply with applicable provisions of NMI 2410.7, this Handbook, and center computer security directives.

(6) Coordinating all functional security requirements with organizations/individuals having procurement, training, or security-related responsibilities (e.g., those having responsibilities in personnel security, physical security, national (including defense-related) security, telecommunications security, information security, internal management control, auditing, quality assurance/control, administrative security, emissions security, and operations security).

c. Identifying DPI's. As illustrated in Exhibits 2-4 and 3-1, the focus of implementing technical requirements begins at the center and DPI levels. Center management is to ensure that all NASA and appropriate NASA contractor computing and telecommunication resources processing NASA information are identified and included under the management of a DPI. A DPI is established by drawing an imaginary boundary around a logical grouping of information, computing, and telecommunications resources for the purpose of managing those resources as an identifiable entity. CCSM's are responsible for assuring that DPI's have been identified. This is accomplished by negotiating with organizations under the cognizance of center management to determine the most logical approach. For example, DPI's might represent logical groupings of information, computing, and telecommunications resources within the boundaries of:

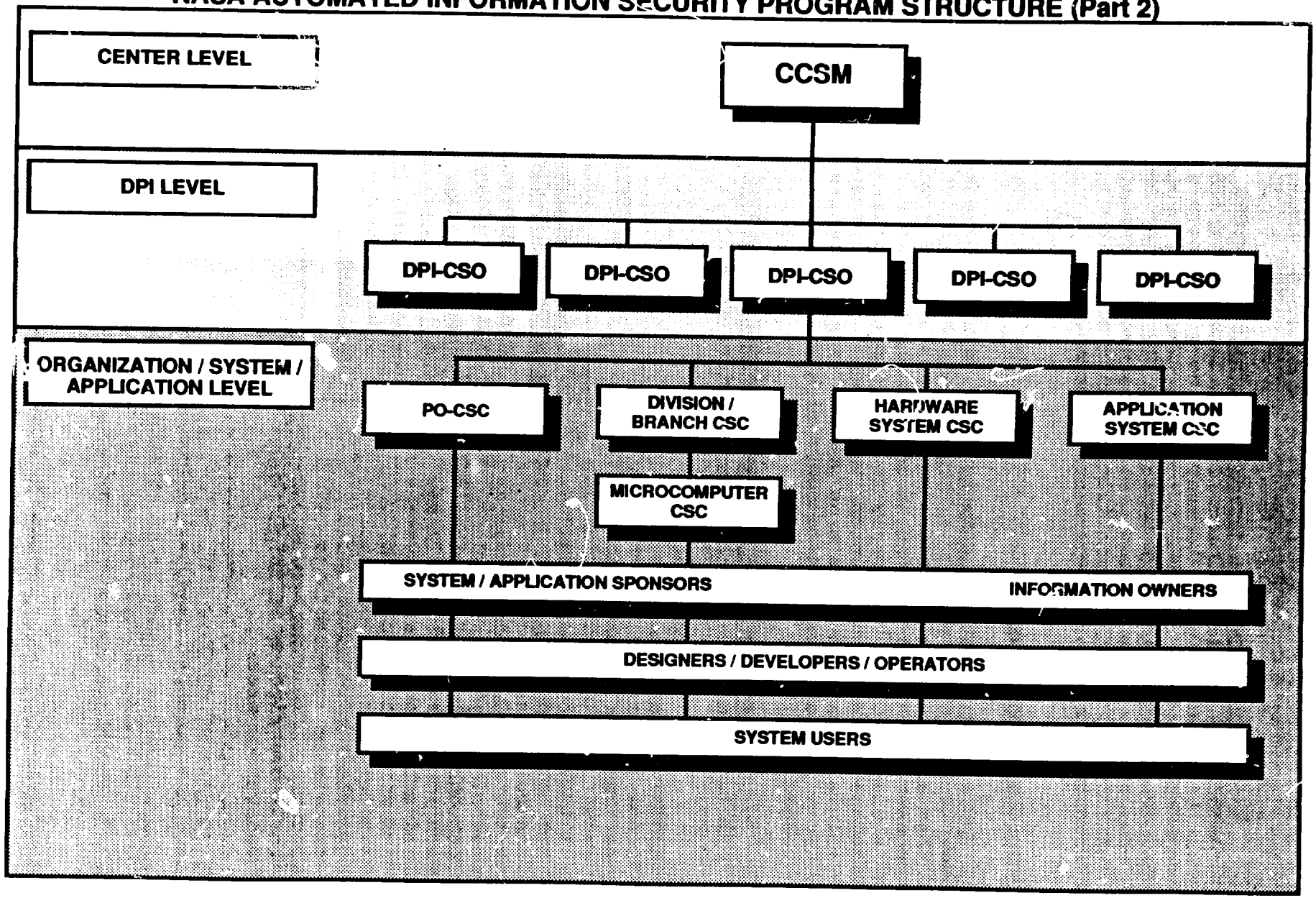
(1) A physical structure at a geographic location (e.g., an entire building or a central computing facility).

(2) An organizational structure (e.g., HQ or center organizational codes).

(3) A combination of these approaches.

The grouping of computer systems for computer security requirements should be consistent, if possible, with that used for DPI's as defined in the Information Technology System Plan (ITSP) submitted annually by each NASA center.

## EXHIBIT 3-1
## NASA AUTOMATED INFORMATION SECURITY PROGRAM STRUCTURE (Part 2)



d. Identifying Additional Entities. DPI-CSO's are responsible for determining if identification of additional entities under the DPI is needed to more effectively manage and coordinate aspects of the DPI computer security program. These entities could represent logical groupings of information, computing, and telecommunications resources associated with sub-elements of the DPI organization, major hardware or software configurations, or clusters of microcomputers.

## 301 DPI REQUIREMENTS

a. Designation of Authorities. Each NASA (or appropriate NASA contractor) manager in charge of a NASA center shall assure that a management official, knowledgeable in both computing and computer security management methods and practices, is designated as the DPI-CSO. Day-to-day security responsibilities may be delegated to technical support personnel. In cases where multiple computer systems or program area applications exist, CSC's may be designated to accomplish specific security responsibilities.

b. DPI-CSO Responsibilities. (See Exhibit 3-2.) The DPI-CSO in coordination with the appropriate CCSM shall:

(1) Implement and administer a management process appropriate to the DPI environment to ensure that sensitivity and/or criticality of information is determined by the application sponsors/owners and that appropriate administrative, technical, physical, and personnel protective measures are incorporated into all new and existing computer systems and applications processing sensitive or mission-critical information to achieve and sustain an acceptable level of security. (See paragraph 302 for a description of this management process.)

EXHIBIT 3-2

| DPI-CSO RESPONSIBILITIES |
| --- |
| • Management Process |
| • Protection Planning |
| • Protection Control |
| • Contingency Planning |
| • Incident Identification |
| • Awareness & Training |
| • Coordination |

(2) Formulate, continually update, and annually review a DPI computer security plan, which will allow the appropriate approving (i.e., DPI) or reviewing (e.g., center and HQ Program Office) authorities to judge the comprehensiveness and effectiveness of the DPI computer security program. In cases where multiple DPI's, computer systems, or program area applications exist, multiple plans may be appropriate. The planning process may also be integrated into center-level planning activities as deemed appropriate by the CCSM. (See paragraph 503 for a description of the required contents of a DPI Computer Security Plan.)

(3) Develop and implement protective measures designed to prevent misuse and abuse of computing resources. (See paragraph 304 for a description of these protective measures.)

(4) Develop and implement a process, as appropriate, for providing contingency planning and reasonable continuity of operations for computer systems and computer applications supporting mission-critical functions. (See paragraph 308 for a description of this process.)

(5) Develop and implement procedures in coordination with the CCSM for identifying computer security incidents and reporting significant computer security incidents, as described in paragraph 309.

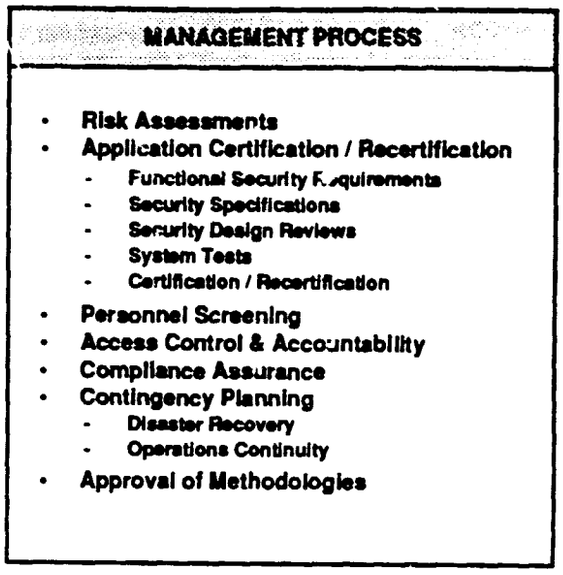
(6) Assure that plans are developed and implemented for conducting continuous CSAT to ensure that NASA and appropriate NASA contractor personnel involved in managing, designing, developing, or maintaining computer applications processing sensitive or mission-critical information, and who use computer systems, are aware of their security responsibilities and know how to fulfill them. This includes being kept aware of vulnerabilities and being trained in techniques to enhance security. (See paragraph 310.)

(7) Coordinate all functional security requirements with organizations/individuals having procurement, training, or security-related responsibilities, e.g., those having responsibilities in personnel security, physical security, national (including defense-related) security, telecommunications security, information security, internal management control, auditing, quality assurance, administrative security, emissions security, and operations security.

## 302 MANAGEMENT PROCESS

The management process must ensure that the following, as a minimum, are carried out (see Exhibit 3-3):

EXHIBIT 3-3




a. Risk Assessments. Periodic risk assessments must be conducted for new and existing DPI's to assure that appropriate, cost-effective protective measures are incorporated and are commensurate with the sensitivity, criticality, and value of associated computer systems, computer applications, and information processed. (See paragraph 303 for a description of the risk assessment process.)

b. Certifying Requirements. Procedures must be established for defining functional security requirements, developing technical security specifications, conducting security design reviews and system tests, certifying and recertifying computer applications processing sensitive or mission-critical information at appropriate phases of the system life cycle, and approving technical security specifications for the acquisition of computing resources or related services. (See paragraph 305 for minimum functional security requirements and certification procedures.)

c. Personnel Screening. Personnel who participate in managing, designing, developing, operating, or maintaining computer applications processing sensitive or mission-critical information, or who access automated sensitive or mission-critical information, must be appropriately screened to a level commensurate with the sensitivity, criticality, or value of the information to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual. Federal personnel are to be screened in accordance with the Federal Personnel Manual, Section 732. Guidance on screening non-Federal personnel is presented in paragraph 306.

d. Access Protection and Accountability. Appropriate protective measures must be established, to the extent economically and technically feasible, for maintaining personal accountability of individual users granted access to sensitive or mission-critical information and for ensuring that they have access to no more information than they are authorized to access.

e. Compliance Assurance. Followup procedures must be in place to assure implementation of protective measures in

accordance with recommendations from compliance review and certification and recertification activities.

f. Contingency and Disaster Recovery Plans. Appropriate disaster recovery plans and contingency plans must be established and maintained to prevent loss of information, minimize interruption, and provide reasonable continuity of computer services should adverse events occur that would prevent normal operations.

g. Approval of Methodologies. Computer security planning, risk assessment, and security certification methodologies shall be approved by appropriate management officials.

303 RISK ASSESSMENT PROCESS

a. NASA recognizes the importance of conducting risk assessments as a basis for making informed management decisions related to accepting identified risk exposures or implementing appropriate cost-effective protective measures to reduce risk exposures to acceptable levels. When used appropriately, risk assessment is a very effective management tool. It should serve to provide a systematic approach for:

(1) Determining the relative value, sensitivity, and criticality of DPI information and computing resources.

(2) Assessing potential threats and perceived risk exposure levels.

(3) Identifying existing protective measures.

(4) Identifying and assessing additional protective alternatives.

(5) Determining acceptability of identified risk levels.

(6) Documenting the assessment process and resulting management decisions.

b. Risk assessments may vary from an informal review of a small-scale microcomputer installation to a formal, fully documented analysis (i.e., risk analysis) of a large-scale computer installation. Since risk assessments can involve many disciplines and organizations, a team approach is recommended, regardless of the size of the systems being analyzed. A tremendous amount of time and effort can be saved by bringing together the right people with the needed knowledge and

experience to review concerns and make subjective judgements, based on professional experience and knowledge.

c. DPI's should continue to be given flexibility for selecting methodologies and implementing risk assessment programs that are most appropriate for their computing environments. However, the risk assessment process must ensure, at a minimum, the following (see Exhibit 3-4):

EXHIBIT 3-4

| RISK ASSESSMENT STEPS |
|---|
| 1. Determine Scope |
| 2. Identify & Value Hardware & Software Assets |
| 3. Identify Information Assets |
| - Determine Sensitivity |
| - Determine Criticality |
| - Determine Value |
| - Determine Potential Adverse Impacts |
| 4. Identify Existing Controls |
| 5. Identify Threats & Estimate Risks |
| 6. Analyze Costs & Benefits Of Potential Controls |
| 7. Recommend Actions |
| 8. Document Actions |
| 9. Followup Review |

(1) A risk assessment methodology is selected (i.e., qualitative, quantitative, or a combination of both) that includes the following elements and logical steps, as appropriate:

(a) Determination of Risk Assessment Scope. For example, a risk assessment may consider an entire DPI, including all hardware, software, and telecommunication aspects, or may be limited to an assessment of an individual mainframe or microcomputer system. Regardless of the approach, the scope of the risk assessment should be planned and maintained within manageable limits, and the level of effort should be commensurate with the nature of the DPI being assessed. For example, a risk assessment of a stand-alone microcomputer installation could be done informally by the owner of the information.

(b) Asset Identification and Value. Identification of major DPI assets and general approximations of their current replacement value in order to establish a basis for making informed decisions on protective measures as described in subparagraph (g) below. For example, if it is known that the approximate value of computing resources within the scope of the risk assessment is about $1 million, it may make sense to spend several hundred dollars or several thousand dollars to enhance protective measures.

(c) Determination of Potential Impacts. General determination of collective sensitivity, criticality, and/or value of information processed or stored at the DPI and potential impacts if information is misused, altered, destroyed, or disclosed. This determination should be based on an analysis of

individual functional security requirements (which are prepared by sponsor/owners) of computer applications processed.

(d) Identification of existing protective measures (i.e., those already in place).

(e) Identification of existing and potential threats and hazards and qualitative estimates of risk exposure and/or quantitative calculations; for example, Annual Loss Expectancy (ALE) associated with potential adverse events.

(f) Determination of acceptable risk exposures, and/or determination of alternative protective measures, associated benefits, and associated costs needed to reduce identified risk exposures and/or ALE to acceptable levels.

(g) Recommendations for accepting risk exposures and/or ALE's, or recommendations for additional appropriate protective measures that are needed to improve security (reducing risk exposure and/or ALE) based on an analysis of the ratio between the estimated cost/benefit of proposed protective measures and the value/sensitivity of information/computing resources requiring protection. The cost of protective measures should not normally exceed a reasonable percentage of the value of assets requiring protection (as identified in subparagraphs (b) and (c)).

(h) Documentation of actions taken or planned as a result of the risk assessment findings and recommendations.

(i) Followup procedures to assure that all actions planned have been carried out.

(2) Risk assessments are performed:

(a) Prior to construction or operational use of a new DPI.

(b) Whenever there is a significant change to an existing DPI.

(c) At periodic intervals, established by the DPI-CSO, that are commensurate with the sensitivity or criticality of the information processed by the DPI, but not to exceed 5 years if no risk assessment has been performed during that time.

(3) The selected risk assessment methodologies and results are approved by appropriate management officials at the center and DPI levels and taken into consideration when certifying or recertifying computer applications processing sensitive or mission-critical information.

(4) Risk assessment results are available for consideration during the evaluation of internal controls, conducted in accordance with NMI 1200.7, "NASA's Internal Control System," that apply to DPI's or computer applications processing sensitive or mission-critical information.

## 304 PROTECTIVE MEASURES TO PREVENT MISUSE AND ABUSE

In addition to other appropriate protective measures (such as those covered in Chapter 4), protective measures to prevent misuse and abuse of computing resources should include the following (see Exhibit 3-5):

a. Developing and implementing a procedure, where technically and economically feasible, to maintain automated computer system logs of access to multiuser computer systems to determine whether unauthorized accesses are being attempted.

EXHIBIT 3-5

| RECOMMENDED PROTECTIVE MEASURES |
| --- |
| • Access Log<br>• Random File Sampling<br>• Awareness Procedures<br>• Incident Response Procedures |

b. Reviewing the contents of computer system files, by means of random sampling, at unannounced intervals.

c. Developing and implementing awareness procedures requiring all personnel who access computer systems to have a working knowledge of computer security ethics, responsibilities, policies, and procedures.

d. Ensuring that all actions constituting suspected or confirmed significant computer security incidents are brought to the immediate attention of the appropriate DPI-CSO; that the extent and cause of any incident is determined; and that reasonable steps are taken to minimize the probability of further incidents including additional training, counseling, disciplinary action, and/or notifying criminal investigative and law enforcement authorities, as appropriate.

## 305 CERTIFICATION PROCESS

Certification is required to provide reasonable assurance that a proposed or significantly changed computer application that processes sensitive or mission-critical information meets all applicable requirements and the original design specifications and that installed protective measures are adequate and functioning properly prior to operational use. The

certification process should involve all those individuals who have participated (or will participate) in the sponsoring, planning, designing, programming, operation, and/or use of the application. Since this process could involve many organizations and individuals, a team approach is recommended. A representative from each functional area should be responsible for witnessing the system test and signing off on his or her area of responsibility. The primary responsibility for accomplishing certification tasks in coordination with the DPI-CSO should reside within the sponsoring/data owner organization. The DPI-CSO of the installation in which the application will be processed should assure that the following process has taken place prior to operational use:

a. New or Modified Applications. For new or significantly changed computer applications that process level 2 through level 3 (as defined in Chapter 4) sensitive or mission-critical information, assure that (see Exhibit 3-6):

(1) Functional security requirements are defined by the system and/or information sponsors/owners based on established installation procedures that include the following:

(a) Identifying and determining the nature of the sensitivity and/or criticality of information to be processed as discussed in Chapter 4 of this Handbook, and determining how the information may be vulnerable to potential threats (e.g., misuse, alteration, destruction, or disclosure);

**EXHIBIT 3-6**

**CERTIFYING NEW / MODIFIED APPLICATIONS**

- **Sponsor / Owner Requirements**
  - **Sensitivity, Criticality & Vulnerability**
  - **Integrity, Availability & Confidentiality**
  - **Potential Impacts**
  - **Acceptable Interruptions / Delays**
  - **Replacement Values**
- **Functional Security Requirements**
- **Technical Security Specifications**
- **Existing Risk Assessments**
- **Design Review & Systems Tests**
- **Certification Document**

(b) Determining primary and secondary system security concerns (i.e., integrity, availability, confidentiality);

(c) Determining potential impacts if sensitive or mission-critical information is misused, altered, destroyed, or disclosed (e.g., embarrassment, legal liability);

(d) Determining when an application that supports a mission-critical function must be back in operation after an interruption to avoid adversely affecting the mission of the user or the sponsoring/owner organization; and

(e) Determining general approximation of replacement values associated with the application/information;

(2) System designers develop technical security specifications that detail functional security requirements and describe how specific protective techniques will be employed. These specifications should be described in technical terms that system developers and programmers can implement;

(3) Functional security requirements and technical security specifications are reviewed and approved prior to acquiring or starting formal development;

(4) Results of risk assessments performed at the DPI in which the computer application will be processed are taken into consideration when defining and approving technical security specifications for computer applications;

(5) Security design reviews and system tests are conducted and approved prior to operational use of computer applications; and

(6) Upon successful completion of the system test, the computer application is certified prior to operational use as meeting requirements of documented and approved functional security requirements, technical security specifications, and related DPI procedures, and that results of the system test demonstrate that the application, computer system, and DPI protective measures are adequate and functioning properly.

b. Recertifications. For operational applications processing sensitive or mission-critical information assure that:

(1) Periodic reviews are conducted and recertifications are made of the continued adequacy and proper functioning of protective measures;

(2) The recertification process takes into consideration all available information (e.g., other reviews and audits that may have been conducted subsequent to the last certification); and

(3) Recertifications are conducted at least every 3 years, as appropriate. Time intervals should be commensurate with the sensitivity/criticality of the information processed. If no significant change has taken place and no deficiencies have

**been identified in other review activities, the recertification process may be less stringent than the initial certification process.**

## 306 PROCEDURES FOR SCREENING NON-FEDERAL PERSONNEL

**Based on requirements in OMB Circular A-130, this procedure has been developed in coordination with the NASA Security Office (HQ Code NIS), which has primary responsibility for establishing policy relating to the screening of all NASA and appropriate NASA contractor (i.e., non-Federal) personnel who participate in the design, development, operation, or maintenance of automated systems, or who access sensitive or mission-critical information. The CCSM, in joint coordination with the Center Security Office, should assure that proper procedures are in place for screening non-Federal personnel.**

a. Scope and Applicability

(1) This procedure provides guidance for the screening of non-Federal personnel who are U.S. citizens and are being granted access to NASA computer systems or the NASA sensitive/critical information they process. For guidance on protecting access by foreign nationals, see paragraph 307.

(2) This guidance need not apply to non-Federal personnel who have or within the last 5 years received a NASA or other Government agency access authorization (or classified clearance) based on a favorable Government-conducted investigation.
Access may be granted by the Center Security Office using an adjudication process.

b. Objective. Personnel screening is to be conducted only to determine an individual's eligibility, or continued eligibility, for access to NASA computer systems or the sensitive/critical information he or she processes. Personnel screening is not to be construed as a determination of suitability for employment.

c. Screening Procedure

(1) The Center Security Office screens Federal employees in accordance with OMB/OPM standards, which require the designation of "position sensitivity levels" for all ADP-computer positions. For screening non-Federal personnel, "position sensitivity levels" are assigned to people, rather than positions, since most non-Federal personnel do not have position descriptions.

(2) Each individual should be screened to a level commensurate with the sensitivity or value of the information to be handled and the risk and magnitude of loss or harm that could be caused by that individual. In general, the level of screening of a non-Federal employee will be influenced by the sensitivity/criticality level of the system the employee will be working on. See Exhibit 3-7 for screening levels.

(3) Personnel screening is a protective measure generally applied based on assessments of other protective measures already in place, potential risk exposures, cost and benefits to be derived, and feasibility of implementation. Functional area managers/sponsors are responsible for designating "position sensitivity levels" to non-Federal personnel. These designations are then forwarded to the Center Security Office. Based on the designated "position sensitivity level" of the non-Federal employee, the Center Security Office will make a determination as to the level of screening required and begin the screening process.

307 CONTROLLING ACCESS BY FOREIGN NATIONALS

a. Introduction. The NASA Office of External Relations has primary responsibility for establishing NASA policy on controlling access to NASA facilities by foreign nationals (i.e., all individuals who are not citizens or nationals of the United States). Refer to NMI 1371.3, "Coordination of Foreign Visitor Activities," for additional information.

b. Purpose. The following policy and procedure has been developed from the perspective of the NASA AIS Program by the Office of IRM in coordination with the Office of External Relations. It sets forth NASA guidelines on controlling electronic access by foreign nationals to NASA computer systems that process sensitive or mission-critical information.

c. Categories. There are two basic categories of foreign nationals that seek access to NASA computer systems: (1) those hired by contractors to perform work tasks in the normal course of business; and (2) those who seek access pursuant to international partnership agreements to conduct work on major multinational projects (e.g., Space Station). Foreign nationals, under category (1) above, that are hired by contractors in the normal course of business, need to be investigated and managed much like other contractor employees. Foreign nationals, under category (2) above, need to be managed consistent with requirements that are negotiated into international partnership agreements.

d. Sponsors. Requests for foreign national access to NASA computer systems must be sponsored by a NASA or another appropriate U.S. Government agency or contractor organization.

## EXHIBIT 3-7
## SCREENING LEVELS FOR NON-FEDERAL EMPLOYEES WORKING WITH COMPUTERS

| AUTOMATED INFORMATION SYSTEM SENSITIVITY / CRITICALITY LEVEL | SCREENING LEVEL* |
|---|---|
| 0 | None |
| 1 | National Agency Check |
| 2 | National Agency Check |
| 3 | Background Investigation |

*Refer to NHB 1610.6 NASA Personnel Security Handbook, Chapter 3 for a description of the screening levels.

e. Submission/Approval of Requests. CCSM shall assure that appropriate procedures are in place to evaluate requests for foreign national access. Requests for foreign national access to NASA computer systems are to be submitted through the appropriate DPI-CSO (i.e., at the installation where primary access will occur) to the Center Security Office for appropriate investigation and approval. Requests for access by foreign nationals from designated areas will be reviewed on a case-by-case basis. Refer to Exhibit 3-8 for additional guidance.

f. Exceptions. Requests for foreign national access which present unusual concerns for a Center's Security Office should be coordinated with the Headquarters Security Office, appropriate Headquarters Program Office, and the Headquarters International Relations Division (Code XIC) for further analysis and concurrence.

## 308 CONTINGENCY AND DISASTER RECOVERY PLANNING

a. Definitions. Disaster recovery plans for DPI's and contingency plans for applications shall provide for minimizing interruptions and reasonable continuity of services if adverse events occur that prevent normal operations. These planning activities may be integrated with each other or other planning activities at the discretion of the CCSM.

(1) Disaster Recovery Plan. Disaster recovery plans are documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a DPI experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with computer application contingency plans, are to provide a reasonable assurance that a DPI can recover from such incidents, continue to process mission-critical applications in a degraded mode (i.e., as a minimum, process computer applications previously identified as most critical), and return to a normal mode of operation within a reasonable time. Such plans are a protective measure generally applied based on assessments of other protective measures already in place, potential risk exposures, costs and benefits to be derived, and feasibility of implementation.

(2) Contingency Plans. Contingency plans describe procedures and identify personnel necessary to respond to abnormal situations and ensure that computer application sponsors/owners can continue to process important applications in the event that computer support at the primary DPI is interrupted

# EXHIBIT 3-8
# MINIMUM INFORMATION
# FOR FOREIGN NATIONAL ACCESS REQUESTS

1. **BACKGROUND DATA**
   - **Personal**
     - Full name.
     - Birthplace.
     - Current citizenship or country.
     - Social Security Number (if available).
   - **Permits**
     - Passport number; place & date of issuance.
     - Visa number & type; place & date issued; expiration date.
     - Alien work permit, if applicable.
   - **Representation**
     - Nationality (Attach documentation).
     - U.S. Government Agency or NASA Center serving as sponsor (Attach documentation).
2. **NATURE OF REQUEST**
   - **Hardware to be accessed**
     - Specific computer system(s).
     - Specific terminal location(s) [Complete address, street, city, state, and dial-in access telephone number].
   - **Files / Applications to be accessed**
     - File / Application names.
     - Level of requested access (READ-only, WRITE, EXECUTE).
     - File owner / Custodian (Name, title & organization) [Attach permission documentation from the data owner and/or application Sponsor].
     - Sensitivity levels of files, application systems, and computer systems.
   - **Access period requested**
     - Commencement-to-end date (Month, day, & year).
     - Termination date (Month, day, & year).
     - Justification (For this particular period).
3. **JUSTIFICATION FOR ACCESS**
   - **Exact nature of assignment requiring access.**
   - **Reasons why hard copy access is insufficient.**
4. **SECURITY CONTROLS TO BE IMPLEMENTED / USED**
   - **Physical access to facilities and hardware.**
   - **File access (i.e., technical controls in the operating system).**
   - **Physical, administrative, and/or online monitoring of the individual.**

(e.g., appropriate automated and/or manual backup capabilities should be considered). These plans are developed in conjunction with computer application or data sponsors/owners and are maintained at the primary and backup data processing installation.

b. Plan Content. Contingency and disaster recovery plans for a DPI should include:

(1) Identification of applications support mission-critical functions. This information should be derived from functional security requirements developed by owners/sponsors.

(2) Potential impacts to the DPI should unnecessary processing delays occur.

(3) When applications must be back in operation after an interruption to avoid adversely affecting the critical missions of the users or the sponsoring/owner organizations. This information should be derived from functional security requirements developed by owners/sponsors.

(4) The relative criticality of each application to the overall mission of the local organization, the center, HQ Program Office, or the Federal agency, and establishing priorities to restore processing support in a logical fashion after an interruption. The relative ranking of applications should be based on recommendations from sponsor/owner organizations and approved by DPI management.

(5) The appropriate amount of documentation. The amount of documentation detailed in these plans should be commensurate with the nature of the DPI (e.g., documented in more detail for large complex DPI's supporting multiuser computer systems and documented in less detail for small DPI's supporting single-user computer systems).

(6) Test intervals and providing reasonable assurance that recovery requirements can be met.

(a) Contingency plans for new applications should be operationally tested at the supporting DPI during initial system tests, and at time intervals commensurate with the associated risk of harm or loss that could be experienced. It is the sponsor/owner organization's responsibility to ensure that a DPI can meet specified functional security requirements. This includes identifying and considering alternative processing DPI's or providing additional funding to enhance protective measures at the supporting DPI.

(b) Disaster recovery plans should be tested at least annually using a cost-effective and reasonable approach.

For example, a limited test based on sample test data from the most critical applications normally provides meaningful results.

(c) Formal written agreements should be established to ensure that sufficient processing capacity and time will be available to meet the recovery requirements of computer applications when backup processing at an alternate DPI is considered necessary.

(7) Identifying key individuals and developing proper emergency notification and response procedures.

309 COMPUTER SECURITY INCIDENT RESPONSE (CSIR) CAPABILITY

a. Responsibilities. Each NASA and appropriate NASA contractor DPI is responsible for establishing a CSIR capability. The CCSM should serve as the primary management point-of-contact and further designate technical support individuals to serve as technical points-of-contact. The CCSM should maintain a listing of all management and technical points-of-contact at DPI's under their cognizance. It is important to formulate strategies and approaches to minimize adverse affects from computer security incidents. A documented, center plan for major incident response, assigning specific responsibilities and including a plan for interacting with the media, is an excellent starting point.

b. Objectives. The following procedure has been developed as a method for timely reporting of significant computer security incidents, for determining the type of information to be reported, and for appropriate follow-on activities after initial notification of an incident. Reports of significant computer security incidents will be used to alert NASA and appropriate NASA contractor DPI's to computer system vulnerabilities, unauthorized access to computer systems, and other problems that could adversely affect any NASA or appropriate NASA contractor site. Sharing incident information can result in vulnerabilities being identified, computer security awareness being elevated, and risk exposures being minimized. The timely reporting of significant computer security incidents also serves to alert NASA management to situations that might affect flight readiness or receive adverse public attention.

c. Procedure Elements. The following procedure provides necessary steps for reporting significant computer security incidents at DPI's that have implemented (or are in the process of implementing) the NASA Automated Information Security Program. Use of this procedure should be compatible with incident and emergency response and reporting procedures that may already be in place.

(1) Immediately after detection of a significant computer security incident (i.e., an incident that could affect other DPI's under the cognizance of the same center), the DPI-CSO should notify the appropriate CCSM. If it is determined that the incident could affect other NASA or NASA contractor installations under the cognizance of the center, an immediate notification should be sent to all appropriate technical points-of-contact. The ultimate objective of this initial notice is to alert other DPI's to potential problems that may impact them. The initial notice should provide the following:

(a) A general description of what occurred.

(b) If appropriate, characterization of perpetrator(s) thought to be involved (i.e., insider, outsider).

(c) What corrective actions are recommended, have been taken, or are planned.

(2) If the CCSM determines that the incident is significant at the center level (i.e., that it could represent significant loss, affect mission readiness, affect other centers, and/or attract public attention), the CCSM should:

(a) Immediately notify the NASA HQ Automated Information Security Program Manager.

(b) Coordinate with all appropriate technical points-of-contact who support the affected constituencies (e.g., UNIX, VAX, MS-DOS, Macintosh, etc.).

(c) Immediately notify the appropriate center CCSM's, who should coordinate with their affected constituencies.

(3) The CCSM, in consultation with the Center Security Office and the DPI-CSO, as appropriate, should determine what type of support (e.g., technical, Inspector General, local law enforcement, FBI, legal, physical or personnel security, classification, and/or public relations) is required. Names and telephone numbers of persons contacted in these organizations should be maintained and included in follow-on reports. Should a classification review determine that an incident affects a classified environment (and therefore, is itself classified), all communications between the DPI, center, Center Security Office, HQ Security Office, and NASA Automated Information Security Program Manager must be through secure channels. (See Chapters 7, 8, and 9.)

(4) After all applicable information has been obtained, a written follow-on report should be forwarded, through the same NASA channels, to the NASA Automated Information Security Program Manager. This follow-on report should contain the minimum information shown in Exhibit 3-9.

(5) A copy of these significant computer security incident reports should be retained by the CCSM and DPI-CSO. The retention period for these records should be determined by the CCSM. Factors to be considered in determining this retention period include the need for availability of this information during periodic security reviews, risk assessments, and trend analysis activities.

(6) The NASA Automated Information Security Program Manager will serve as the main point-of-coordination among NASA center senior management, NASA HQ Program Offices, NASA senior management, and external organizations.

(7) The center closest to the occurrence of a significant computer security incident should assume a lead role in developing accurate reports of related facts and coordinating public releases of information with the local Public Relations Office, the NASA Automated Information Security Program Manager, and Headquarters Public Affairs, Code P.

d. Non-duty Hours Considerations. Current listings should be maintained of emergency situations and designated NASA CSIR management officials to be notified. The listing should be complete with after-hours phone numbers and designated alternates for each official. These procedures should be integrated, as appropriate, with local procedures for after-hours incident response. Emergency situations after-hours that require immediate HQ involvement should be directed to the Goddard Space Flight Center (GSFC) Emergency Console. Calls will then be forwarded to the responsible management official.

## 310 COMPUTER SECURITY AWARENESS AND TRAINING (CSAT)

a. Continuous CSAT. Continuous CSAT is required at centers and DPI's to sustain the effectiveness of the NASA Automated Information Security Program. Employees who understand their responsibilities, the need for security, and what they must do to promote it are one of the best protections against computer security incidents. Therefore, training should be provided on an ongoing basis to employees and contractors, as appropriate. New employees should receive awareness training during their initial orientation. Refresher training should be offered at least annually. Additional training will be required whenever there are major changes in a computing environment or the protective measures baseline.

# EXHIBIT 3-9
# MINIMUM INFORMATION FOR FOLLOW-ON INCIDENT REPORT CONTENT

1. DATE AND TIME OF INCIDENT

2. LOCATION OF INCIDENT: DPI and/or appropriate identification of affected hardware and software.

3. NATURE OF THE INCIDENT
   - A. What caused the incident.
   - B. Characterization of perpetrator(s) thought to be involved (i.e., insider, outsider).
   - C. Sensitivity level of information involved*.

4. EFFECTS OF THE INCIDENT
   - A. Organizational element affected.
   - B. What is affected [e.g., computer center, hardware, communication networks, software (including version number)].

5. CORRECTIVE ACTIONS TAKEN OR PLANNED

6. TECHNICAL SUPPORT, LAW ENFORCEMENT, LEGAL COUNSEL, SECURITY, CLASSIFICATION, AND PUBLIC RELATIONS CONTACTS MADE, AS APPROPRIATE

7. WHAT IMPLICATION DOES THIS INCIDENT HAVE FOR OTHER SITES, IF ANY, AND WHICH OTHER SITES HAVE BEEN NOTIFIED

8. RECOMMENDATIONS CONCERNING THE FOLLOWING
   - A. Assistance needed by the DPI.
   - B. Need to change or establish new policies and/or procedures.
   - C. Additional action that should be taken by higher authorities.

9. NAME AND TELEPHONE NUMBER OF LEAD DPI-CSO

10. NON-DUTY HOUR ACTIONS, IF ANY
    - A. Time and name of NASA Duty Officer contacted.
    - B. Determinations made.
    - C. Actions taken.

* For an incident involving NASA classified information, include the incident ranking (see Chapter 8).

b. Multifaceted Approach. NASA has a multifaceted approach (e.g., top-down and bottom-up, internal and external sources, etc.) to CSAT. It is believed that an effective CSAT program must offer more to personnel than just an hour of classroom training once a year or a limited selection from NASA-sponsored training activities. The training should incorporate a variety of instructional approaches and be appropriate for the target audience. To this end, NASA sponsors many internal security conferences, seminars, workshops, and meetings which are considered part of the overall NASA CSAT Program. NASA encourages personnel to seek both internal and external CSAT sources to meet specific job-related needs. Sources available include:

(1) Annual NASA-Specific Conference. The IRM Office sponsors an annual computer security conference that is specific to NASA computing environments. This conference provides a forum for and promotes interaction among (NASA employee and NASA contractor) computer security representatives from NASA HQ, centers, and DPI's. It also facilitates the exchange of technical and management information related to protecting computer systems and automated information throughout the NASA community.

(2) Annual CCSM Working Group Sessions. The IRM Office sponsors at least two CCSM Working Group Meetings per year for the purpose of bringing all CCSM's together to share current information, solve common problems, and plan future NASA Automated Information Security Program management strategies.

(3) NASA Electronic Computer Security Bulletin Board. The IRM Office, with administrative support from the HQ Office of Space Flight, sponsors a NASA bulletin board service on NASAMAIL for the purpose of sharing current management and technical information related to computer security within the NASA and the NASA contractor community.

(4) Periodic Computer Security Highlight Articles. The IRM Office publishes "IRM Highlights" on a weekly basis. This publication contains timely articles on all aspects of IRM and normally includes articles on computer security. Articles on computer security are made available on the NASAMAIL Computer Security Bulletin Board. Centers are encouraged to disseminate this information to cognizant DPI's or extract information to enhance their own periodic publications that are disseminated to raise security awareness of current issues.

(5) Ongoing DPI Training. CSAT is required to sustain the effectiveness of the NASA Automated Information Security Program. Flexibility is given to allow this training to be

conducted in a manner that is cost-effective and appropriate for a DPI. Some options include:

(a) Formal Classroom Training.
(b) Self-Instruction Courses.
(c) Computer-Assisted Instruction (CAI).
(d) Movies (16 mm).
(e) Videotapes.
(f) Newsletters and Bulletins.

(6) Ongoing Training from External Sources. NASA and NASA contractor personnel are encouraged to evaluate their specific CSAT needs and seek additional generic and specialized training from external sources (e.g., OPM, GSA, Department of Agriculture Graduate School, DOD Computer Institute, National Computer Security Center, and commercial vendors).

(7) Significant Incident Reporting (Feedback Loop). Reports of significant incidents are used to alert other centers and DPI's to potential threats and other problems that could adversely affect their operations. Through the sharing of incident information NASA management can be kept informed, national trends can be determined, computer security awareness can be elevated, and potential risk exposures minimized.

(8) Sharing of Security Tools and Techniques. The NASA Automated Information Security Program establishes a network of computer security contacts at all organizational levels. Individuals at all levels are encouraged to establish professional working relationships with their counterparts for the purpose of improving communications and sharing effective computer security tools and techniques. Such relationships are vital to reduce burden, solve common computer security problems, and provide effective response during significant incident situations. The IRM Office encourages all centers to continually submit effective management tools and technical techniques they have developed for dissemination to other centers for evaluation and implementation consideration.

## 311 PROCUREMENT OF PRODUCTS AND SERVICES

The Office of Procurement (Code H) has primary responsibility for developing policy and guidance related to NASA procurements. The following guidance has been developed by the IRM Office from the NASA Automated Information Security Program perspective in coordination with the Office of Procurement.

a. Introduction. Functional security requirements must be developed by sponsors/owners to integrate appropriate security protective measures into hardware, software, telecommunications, or supporting contractor services. Also, detailed technical

security specifications must be developed by designers. These requirements (e.g., risk assessment, technical hardware/software measures, design reviews, system tests, certification prior to operational use, personnel screening, CSAT) must be included in technical specifications and solicitations/contracts.

b. NASA Contracting Environment. Due to the nature of NASA operations, NASA has virtually every type of contractual situation for the acquisition of computer products and related support services. Because of the diverse range of procurement and contractual situations and the degree of management that may exist between NASA and any given contractor, a reasonable approach must be taken. Procurement and contractual situations must be evaluated on a case-by-case basis in order to avoid imposing unnecessary constraints on contractors that are not under the direct management of NASA.

c. Project Manager Responsibilities. The DPI management official (e.g., the Project Manager or the Contracting Officer's Technical Representative (COTR)) is responsible for assuring that appropriate functional security requirements, technical security specifications, and methods for evaluating security adequacy are included in solicitation documents.

d. Sponsoring Organization Responsibilities. Functional security requirements and technical security specifications shall be developed and approved by sponsors of the acquisition and reviewed by the designated DPI-CSO. General guidance for some types of functional security requirements are included in GSA's FIRMR. Other DPI-specific requirements will have to be developed based on the protective techniques selected as the result of a risk assessment and further guidance, which may be provided by NASA procurement offices, GSA, and NIST. To the extent feasible, functional security requirements should be stated in functional terms (i.e., "what" is needed) relative to security objectives. This will permit the DPI to benefit from new technology or an innovative application of existing technology.

e. Contracting Officer Responsibilities. For the procurement of computing resources or related support services, contracting officers shall:

(1) Ensure that no action is taken on a request for proposal or procurement for computing resources or related support services unless appropriate functional security requirements and specifications are included in accordance with established DPI procedures.

(2) Ensure that NASA technical proposal instructions include a statement requiring a detailed outline and demonstration of the offeror's computer security capabilities

that comply with the functional security requirements of the solicitation and contract.

(3) Include a clause in solicitations and contracts requiring the contractor to comply with the functional security requirements set forth in applicable parts of NMI 2410.7 and this Handbook.

f. Evaluating Security Capabilities. Proposal evaluators shall review the offeror's proposed approach and witness live test demonstrations, as appropriate, to evaluate the adequacy of protective measures and the capability of the offeror to meet the functional security requirements and technical security specifications contained in the solicitation and contract. Exceptions to live test demonstrations will be considered in cases where it may be determined to be cost prohibitive. Proposal evaluators shall then certify, if appropriate, the adequacy of the offeror's compliance. This certification shall be obtained by the contracting officer before proceeding with the procurement.

g. Contract Administration. CCSM's and DPI-CSO's shall conduct in coordination with their Contracting Officer, COTR, and Project Managers, periodic reviews of contracts in progress to ensure continued compliance with functional security requirements. All instances of noncompliance shall be reported to the Contracting Officer or designated representative.

h. Requirements for Contractor-Operated DPI's. As indicated in paragraph 102, the provisions of this Handbook apply to support contractor organizations as provided by law and/or contract, and as implemented by the appropriate contracting officer. The center and DPI management processes should assure that, in contracts for equipment, software, the operation of DPI's, or related services:

(1) Appropriate functional security requirements and specifications are included in procurement specifications and/or statements of work.

(2) Functional security requirements and technical security specifications are reasonably sufficient for the intended application; that they comply with established DPI procedures; and that protective provisions at the acquired DPI are adequate and functioning properly prior to operational use.

(3) Resource-sharing service agreements provide for compliance with applicable provisions of NMI 2410.7 and this Handbook by responsible management officials at the acquired processing DPI.

# CHAPTER 4. AUTOMATED INFORMATION CATEGORIES AND SENSITIVITY/CRITICALITY LEVELS

## 400 INTRODUCTION

There are two important concepts covered in this Chapter. The first concept is that there are reasonably definable "categories" of information, each with its own unique management and security concerns. The second is that once automated information has been categorized, it is necessary to determine a relative sensitivity and/or criticality level for that information, so appropriate protective measures can be considered and a protective measures baseline established for supporting software, hardware, and telecommunication systems. The technical depth of a risk analysis, type and frequency of security awareness training, and the requirement for incident reporting are all examples of areas where increasing sensitivity level should cause increased emphasis and resource expenditures.

a. Information Categories. Information categories are simply logical groupings of information that are based on a legal requirement, a policy requirement, or a management concern to treat a category of information in a particular way. An understanding of these categories is the first step in determining the nature of the sensitivity and/or criticality of automated information and the types of protective measures that may be appropriate when the information is processed by a computer system or transmitted over a telecommunications network. In order to assist application sponsors and information owners with the sometimes subjective task of identifying the nature of sensitive automated information and identifying automated information that supports mission-critical functions, NASA has developed a method for categorizing automated information (as illustrated in Exhibit 4-1). All information falls into one or more of these categories.

# EXHIBIT 4-1
# NASA AUTOMATED INFORMATION CATEGORIES

| CATEGORY | | EXPLANATION |
|---|---|---|
| # | NAME | |
| 1 | INFORMATION ABOUT PERSONS | Information related to personnel, medical, and similar information. All information covered by the Privacy Act of 1974 falls into this category. |
| 2 | FINANCIAL, COMMERCIAL, AND TRADE SECRET INFORMATION | Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary). Also included in this category are payroll automated decision-making procurement, inventory, and other such financially-related systems. |
| 3 | NASA INTERNAL OPERATIONS | Information related to the internal operations of NASA. This category includes personnel rules, bargaining positions, and advance information concerning procurement actions. |
| 4 | INVESTIGATION, INTELLIGENCE-RELATED, AND SECURITY INFORMATION | Information related to investigations for law enforcement purposes, intelligence-related information that cannot be classified, but is subject to confidentiality, and extra security controls. Includes detailed security plans, but does not include general plans, policies, or requirements. |
| 5 | OTHER FEDERAL AGENCY INFORMATION | Information that is required by statute or another Federal agency. This category includes information that is not the primary responsibility of NASA. |
| 6 | UNCLASSIFIED NATIONAL SECURITY-RELATED INFORMATION | National defense and intelligence-related information subject to the policy, procedural, and protection requirements established under National Security Decision Directive (NSDD) 145 by the National Telecommunications and Information Systems Security Committee. |
| 7 | NATIONAL RESOURCE SYSTEMS INFORMATION | Information related to the protection of a national resource (e.g., the Space Shuttle and related support systems). |
| 8 | MISSION-CRITICAL INFORMATION | Information that has been designated as critical to a NASA mission. |
| 9 | OPERATIONAL INFORMATION | Information that requires protection during operations. This is usually time-critical information. |
| 10 | LIFE-CRITICAL INFORMATION | Information critical to life-support systems (i.e., information whose inaccuracy, loss, or alteration reasonably could be expected to result in loss of life). |
| 11 | HIGH OR NEW TECHNOLOGY INFORMATION | Information relating to high or new technology prohibited from disclosure to certain foreign governments, or that may require an export license from the Department of State and/or the Department of Commerce. |
| 12 | OTHER UNCLASSIFIED INFORMATION | Any information for which there is a management concern related to its adequate protection, but does not logically fall into one or more of the above 11 categories . Use of this category should be rare. |
| 13 | CLASSIFIED NATIONAL SECURITY-RELATED INFORMATION | Information classified for national defense purposes (i.e., under E.O. 12356). |

b. Sensitivity/Criticality Levels. NASA has established four hierarchical "levels" of sensitivity/criticality to assist application sponsors, information owners, system designers, and system developers (see Exhibit 4-2). All automated information falls into one of these four sensitivity/criticality levels, in

## EXHIBIT 4-2
## NASA UNCLASSIFIED AUTOMATED INFORMATION SENSITIVITY / CRITICALITY LEVELS

| AUTOMATED INFORMATION SENSITIVITY / CRITICALITY LEVEL | EXPLANATION<br>AUTOMATED INFORMATION, AUTOMATED APPLICATIONS, OR COMPUTER SYSTEMS THE INACCURACY, ALTERATION, DISCLOSURE, OR UNAVAILABILITY OF WHICH: |
|---|---|
| 0 | • Would have a **NEGLIGIBLE** impact on NASA's missions, functions, image, or reputation. The impact, while unfortunate, would be insignificant and almost unworthy of consideration; or<br>• Probably would **NOT** result in the loss of a tangible asset or resource. |
| 1 | • Would have a **MINIMAL** impact on NASA's missions, functions, image, or reputation. A breach of this sensitivity level would result in the least possible significant unfavorable condition with a negative outcome; or<br>• Could result in the loss of **SOME** tangible asset or resource. |
| 2 | • Would have an **ADVERSE** impact actively opposed to NASA's missions, functions, image, and reputation. The impact would place NASA at a significant disadvantage; or<br>• Would result in the loss of **SIGNIFICANT** tangible asset(s) or resource(s). |
| 3 | • Would have an **IRREPARABLE** impact permanently violating the integrity of NASA's missions, functions, image, and reputation. The catastrophic result would not be able to be repaired or set right again; or<br>• Would result in the loss of **MAJOR** tangible asset(s) or resource(s) including posing a threat to human life. |

which each level has a generic set of protective measure considerations (as illustrated in Exhibit 4-3). The following paragraphs describe the 13 automated information categories, the four sensitivity/criticality levels, and the protective measure considerations for each level.

## 401 INFORMATION CATEGORIES

a. As shown in Exhibit 4-1, NASA has defined 13 categories of information to facilitate managing automated information. The predominant statutory bases for these categories are:

(1) Federal Managers Financial Integrity Act of 1982 (Public Law 97-255; 31 U.S.C. 66a).

(2) Paperwork Reduction Act of 1980 (Public Law 96-511; 44 U.S.C. 3501).

(3) Freedom of Information Act of 1974 (Public Law 93-502; 5 U.S.C. 552b).

(4) Privacy Act of 1974 (Public Law 93-579; 5 U.S.C. 552a).

b. Categories 1-5 are derived from the statutes indicated above in subparagraph a and apply to all Federal agencies. Category 6 is derived from guidance in NSDD 145. Categories 7-12 are derived from assorted Federal directives. Category 13 is derived from Presidential Executive Order (E.O.) 12356. The categories are defined in the following paragraphs.

(1) Information About Persons (Category 1). This category includes information related to personnel, medical, and similar information. All information covered by the Privacy Act of 1974 falls into this category.

(2) Financial, Commercial, and Trade Secret Information (Category 2). Category 2 includes information from applications such as financial, procurement, inventory, and decision making. It also includes commercial information received in confidence, trade secrets, and proprietary information.

(3) NASA Internal Operations (Category 3). This incudes information related to the internal operations of NASA. This category includes certain personnel rules, bargaining positions, advance information concerning procurement actions, etc.

## EXHIBIT 4-3
## PROTECTIVE MEASURE CONSIDERATIONS (Part 1)

| LEVEL OF SENSITIVITY / CRITICALITY / PROTECTION CATEGORY | LEVEL 0 Considerations | LEVEL 1 (All level 0 considerations plus:) |
|---|---|---|
| ACCESS CONTROL | User identification and passwords to uniquely identify each person.<br>Maintain log of all accesses to multi-user systems. | Physical, procedural, or technical controls that allow physical and/or logical control over authorization for and access to the system and processing resources. |
| CONFIGURATION MANAGEMENT | Catalog of all files.<br>Licenses for all software used. | A configuration management process that controls changes to any security-related and sensitive software, hardware, or procedure for the system. |
| BACKUP COPIES OF SOFTWARE | At least one generation of backup application software. Monthly backups of changed data files. | At least two generations of backups with the oldest generation being stored at a location other than the immediate vicinity of the system. |
| PHYSICAL ACCESS | Physical security required when the computing resources are unattended. | Systems physically protected to prevent unauthorized access, theft, or destruction. Physical key locks for microcomputer fixed/hard disks. Separate locks should also be used to prevent hardware theft. |
| NETWORK ACCESS | | Passwords required to access any network. When doing file transfers, error checking/correction software required. |
| PERSONNEL SECURITY | All users trained in automated applications they use, proper software handling procedures, and basic computer security. | National Agency Check (NAC) Screening. |
| ENVIRONMENTAL CONTROLS | Proper dust, water, temperature, humidity, and ventilation controls required. Also, power surge protection required. | |
| STORAGE MEDIA | Proper storage bins or containers required for data storage media. | |
| COMMUNICATIONS | Communications links will be approved by the responsible CCSM(s) prior to implementation. | |
| AUDIT TRAILS | | |
| LOGOFF / TIME OUT FEATURES | | |
| DATA BASE MANAGEMENT SYSTEMS | | |
| INFO & APPLICATION PROTECTION | Random unannounced reviews of system files. | |
| CONTINGENCY/ DISASTER RECOVERY PLANS | | Contingency and Disaster Recovery Plans should be developed in accordance with paragraph 308. |

## EXHIBIT 4-3
## PROTECTIVE MEASURE CONSIDERATIONS (Part 2)

| LEVEL OF SENSITIVITY/ CRITICALITY / PROTECTION CATEGORY | LEVEL 2 (All level 0 and 1 considerations plus:) | LEVEL 3 (All level 0, 1, and 2 considerations plus:) |
|---|---|---|
| ACCESS CONTROL | Protection measures that allow for:<br>• Identification and authentication of individual users;<br>• Restriction of functional capabilities of individual users;<br>• Users to control access of other individual users to their data and applications; and<br>• Data encryption. | Controls that can at all times restrict and log individual user access by system resource, application, and data files. Authorization to access system resources, applications, and data files must be confirmed by the sponsors/owners (reconfirmation every 6 months).<br>Non-use of encryption justified. |
| CONFIGURATION MANAGEMENT | | Controls are in place that allow data bases to be stored off-line. |
| BACKUP COPIES OF SOFTWARE | | |
| PHYSICAL ACCESS | | |
| NETWORK ACCESS | On Selected Systems: Written consent, identifying other network nodes authorized to access the system node obtained from the responsible DPI-CSO prior to enabling any network connection. | Written consent, identifying other network nodes authorized to access the system node obtained from the responsible DPI-CSO prior to enabling any network connection. |
| PERSONNEL SECURITY | National Agency Check Screening | Background Investigation (BI) Screening |
| ENVIRONMENTAL CONTROLS | | |
| STORAGE MEDIA | | |
| COMMUNICATIONS | A well-defined/described path for the initial user identification and authentication processes.<br>Data encryption on selected systems. | No uncontrolled dial-up access or unauthorized connections to external networks.<br>Non-use of encryption justified. |
| AUDIT TRAILS | System generation of journals or audit logs, of access to the system and to information and applications at the individual user level. | |
| LOGOFF / TIME OUT FEATURES | System logoff of work stations that have not been in communication with the Central Processing Unit (CPU) for a period of time determined by installation management. | |
| DATA BASE MANAGEMENT SYSTEMS | Systems to provide for the integrity, confidentiality, and availability of all information resident in the data base. The data base administrator is responsible for ensuring that sponsors/owners are informed and concur in all defined access privileges to and uses of their information. | |
| INFO & APPLICATION PROTECTION | | Sensitivity level indicators will be associated with all system resources, information, and applications at all times. |
| CONTINGENCY/ DISASTER RECOVERY PLANS | | |

(4) Investigatory, Intelligence-Related, and Security Information (Category 4). This category includes information related to police intelligence and/or law enforcement investigations or informants. It also includes some computer security information (such as detailed security plans for the protection of systems and specific automation vulnerabilities). Note that this category does not include general plans, policies, or requirements, nor does it include Federal or national security intelligence information.

(5) Other Federal Agency Information (Category 5). Other Federal agency information includes information whose gathering and/or maintenance is required by statute or another Federal agency. Information in this category is not the primary responsibility of NASA. For example, this category would include DOD or Department of Energy (DOE) information processed in NASA computers for DOD or DOE, respectively.

(6) Unclassified National Security-Related Information (Category 6). This category includes national defense and Federal intelligence-related information subject to the policy, procedural, and protective requirements established by the National Telecommunications and Information Systems Security Committee (NTISSC). This information may require protection in addition to that required under NASA guidance. This information is not classifiable under E.O. 12356, but requires protection in accordance with NTISSC policy.

(7) National Resource System Information (Category 7). This is information related to the protection of a national resource (such as the Space Shuttle or the Space Station Freedom.)

(8) Mission-Critical Information (Category 8). This is information that has been designated as critical to the NASA mission.

(9) Operational Information (Category 9). This is information that requires protection during operations. It is usually time-critical information.

(10) Life-Critical Information (Category 10). This is information critical to life support systems (i.e., information whose inaccuracy, loss or alteration reasonably could be expected to result in loss of life).

(11) High or New Technology Information (Category 11). This is information relating to high or new technology prohibited from disclosure to certain foreign governments or may require an export license from the Department of State and/or the Department of Commerce.

(12) Other Unclassified Information (Category 12). This is any information that does not logically fall into one or more of the 11 categories and that is not classified for national security purposes. Use of this category should be very rare.

(13) Classified National Security-Related Information (Category 13). This is information classified for national security purposes (i.e., under E.O. 12356). All computer security actions related to this category are covered in Chapters 7, 8, and 9 of this Handbook.

## 402 SENSITIVITY/CRITICALITY LEVELS

a. Introduction. The sensitivity levels defined in Exhibit 4-2 are based on the amount of harm or loss that could be experienced from an adverse event that affects the availability, integrity, or confidentiality of NASA computing or information resources. A hypothetical relationship between the automated information categories and sensitivity/criticality levels is presented in Exhibit 4-4 for general guidance only. Detailed analyses should be conducted by information sponsors and owners, on a case-by-case basis, and should be reviewed by a DPI-CSO before making any final sensitivity and/or criticality determinations. The sensitivity/criticality of automated information should also be periodically re-evaluated, as the influencing factors change.

b. Automated Information and Applications. The sensitivity and/or criticality of automated information is determined by applicable sponsors and information owners. A sensitivity and/or criticality level should also be assigned to each automated application, based on the sensitivity and/or criticality of the automated information the application will process. The sensitivity/criticality level of an automated application is at least as high as the most sensitive/critical automated information that will be processed by that application. The internal formulas or the information editing criteria in the application source code could raise the sensitivity/criticality level of the application even higher than the information it handles.

c. Computer Systems. DPI-CSO's should assign each NASA computer a sensitivity/criticality level, based on the sensitivity/criticality level of the applications processed on each computer system. Each computer system should have a sensitivity/criticality level that is at least as high as that of the most sensitive/critical application processed. However,

## EXHIBIT 4-4
## CATEGORIES AND SENSITIVITIES

| INFORMATION CATEGORY | TITLE | MINIMUM SENSITIVITY LEVEL | | | |
|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 |
| 1 | Personal | | ● | | |
| 2 | Financial, Commercial, and Trade Secret | | | ● | |
| 3 | NASA Internal Operations | | ● | | |
| 4 | Investigatory, Intelligence-related, and Security | | | | ● |
| 5 | Other Federal Agency | | ● | | |
| 6 | Unclassified National Security-Related | | | ● | |
| 7 | National Resource Systems | | | ● | |
| 8 | Mission-Critical | | | | ● |
| 9 | Operational | | | ● | |
| 10 | Life-Critical | | | | ● |
| 11 | High or New Technology | | | ● | |
| 12 | Other Unclassified | ● | | | |

NOTE: Category 13, Classified Information, is covered in Chapters 7 through 9.

significant replacement costs, unusually large numbers of applications supported, and/or an unusually large volume of information processed can raise the sensitivity/criticality level of a computer system even higher than the sensitivity/criticality level of the most sensitive/critical application processed on that system.

## 403 PROTECTIVE MEASURE BASELINE CONSIDERATIONS

Protective measure considerations for each sensitivity and/or criticality level are presented as general guidance in the following paragraphs. The selection or omission of protective measures should be justified and based on the results of a risk assessment. DPI's may elect to increase their protection, add additional protective measures, or establish a mandatory minimum protective measures baseline, as they deem appropriate. (See Exhibit 4-3. Also, see paragraph 304.)

a. Sensitivity/Criticality Level 0. Sensitivity level systems should provide for adequate protection of information through the following protective measures:

(1) Access Protection. Whenever a single computer system is used by more than one person (whether or not that use is concurrent), physical, procedural, and technical protective measures should be provided that allow for identification and authentication of individual users and to prevent access by unauthorized persons.

(2) Configuration Management. All files should be cataloged and there should be licenses for all software used.

(3) Back-up Copies of Software. At least one generation of backup software should be maintained. Backups of changed information files should also be maintained.

(4) Physical Access. Physical security (such as door locks and cable locks) should be required when the automated information resources are unattended.

(5) Personnel Security. All users of computer systems should be trained in the automated applications they use, proper software handling procedures, and basic computer security practices.

(6) Environmental Measures. Proper environmental measures (to minimize the impacts of dust, water, temperature, humidity, and ventilation) should be required. Also, power surge protection should be required for hardware.

(7) Storage Media. Proper storage bins or containers should be required for information storage media (e.g., disks, tapes, etc.).

(8) Communications. The communications links connecting the computer system to other systems, networks, workstations, or terminals should be approved by responsible management prior to the implementation of the connection.

b. Sensitivity/Criticality Level 1. Sensitivity level 1 systems should provide all Sensitivity level 0 protective measures as well as:

(1) Access Protection. Physical, procedural, or technical protective measures should be provided that allow physical and/or logical management of authorization and access to the system and processing resources.

(2) Configuration Management. A configuration management process should be developed and maintained that monitors changes to any security-related and sensitive software, hardware, or procedure for the system.

(3) Back-up Copies of Software. At least two generations of back-ups should be maintained, with the oldest generation being stored at a location other than the immediate vicinity of the system.

(4) Physical Access. Systems should be physically protected to prevent unauthorized access, theft, or destruction. Physical key locks should be used on microcomputer fixed/hard disks. Separate physical locks should also be used to prevent hardware theft.

(5) Network Access. Passwords should be required for access to or from any network. Use of software that provides error checking and some error correction capability should be required when performing file transfers using networks.

(6) Contingency and Disaster Recovery Plans. Contingency Plans for applications and Disaster Recovery Plans for computer installations should be developed to provide for minimal interruptions and reasonable continuity of services. These plans should be developed in accordance with paragraph 308.

c. Sensitivity/Criticality Level 2. Sensitivity level 2 systems should implement the protective measures required for sensitivity levels 0 and 1, in addition to the following:

(1) Access Protection. Physical, procedural, and technical protective measures should be provided that allow for:

(a) Restriction of the functional capabilities of individual users.

(b) Ability for individual users to manage access (e.g., read, modify, or delete) by other individual users to their information and applications.

(c) Consideration of encryption of stored data.

(2) Audit Trails. The system should provide for the generation of journals, or audit logs, of accesses to the system and to information and applications at the individual user level. Access to journals and audit logs should be restricted to a well-defined group of users authorized by DPI management.

(3) Communications. All communication paths for the system should be described, and a well-defined path should exist for the initial user identification and authentication processes. Encryption of data to be transmitted should be evaluated by sponsors/owners.

(4) Network Access. Written consent, identifying other network nodes authorized to access the system node, should be obtained from responsible DPI management prior to enabling any network connection or interconnection.

(5) Logoff/Time Out Features. The system should logoff work stations that have not been in communication with the CPU for a period of time determined by DPI management.

(6) Data Base Management Systems (DBMS's). DBMS's should provide for the integrity, confidentiality, and availability of all information resident in the data base. Individuals responsible for data base administration are responsible for ensuring that information owners are informed of and concur in all defined access privileges to and uses of their information.

d. Sensitivity/Criticality Level 3. Sensitivity level 3 systems should implement the minimum protective measures required for sensitivity levels 0, 1, and 2, in addition to the following:

(1) Access Protective Measures. Access protective measures should be provided that can at all times restrict and log individual user access by system resource, application, and information files. Authorization to access system resources, applications, and information files must be confirmed by the information owners and shall be reconfirmed periodically, but at least every 6 months.

(2) Information and Application Labels. Sensitivity level indicators should be associated with computing resources, applications, and information while Level 3 sensitive information is being processed.

(3) Configuration Management. Protective measures should be in place to allow data bases to be stored offline.

(4) Communications. There should be no uncontrolled dial-up access or unauthorized connections to external networks. Management decisions not to use data encryption should be justified. Threats and risks associated with connections to wide-area and/or internationally linked networks shall be evaluated by sponsors/owners, and the resulting management decisions should be justified.

# CHAPTER 5. COMPUTER SECURITY PLANNING

## 500 INTRODUCTION

This Chapter presents details of the required computer security planning activities. Specifically, it covers the NASA Automated Information Security Program Plan, the NASA HQ Program Office Computer Security Plan (PO-CSP), the Center Computer Security Plan (CCSP), the DPI Computer Security Plan (DPI-CSP), and Contingency Plans. A discussion of how NASA complies with external requests for planning information is found in paragraph 505.

## 501 HEADQUARTERS COMPUTER SECURITY PLANNING

### a. NASA Automated Information Security Program Plan

(1) Scope. The NASA Automated Information Security Program Plan is agencywide in scope. It does not provide detailed planning information for any particular center, computer system, or automated application. However, it documents goals, objectives, agencywide program management strategies, agencywide computer security awareness and training strategies, and approaches for conducting management reviews to ensure optimal levels of security are sustained.

(2) Purpose. The purpose of the NASA Automated Information Security Program Plan is to document the overall NASA Automated Information Security Program goal, objectives, directions, and strategies for the NASA Automated Information Security Program Manager.

(3) Manager. The NASA Automated Information Security Program Manager is responsible for developing, implementing, monitoring, and evaluating this plan.

(4) Distribution. The NASA Automated Information Security Program Plan shall be distributed to all NASA CCSM's and PO-CSM's.

(5) Publication Date. The NASA Automated Information Security Program Plan shall be revised annually and published by October 1.

(6) Period Covered. The NASA Automated Information Security Program Plan details the computer security accomplishments of the past fiscal year, as well as the plans for

the current budget year plus one. Thus, it covers a total of 3 years.

(7) Relationship with Other Plans

(a) The NASA Automated Information Security Program Plan provides input for national computer security submission requirements from OMB and NIST. PO-CSP's, CCSP's, and DPI-CSP's should operate within the NASA Automated Information Security Program goal and objectives, as defined in the NASA Automated Information Security Program Plan.

(b) Major security activities reported in the Program Office and center computer security plans should be reflected in the NASA Automated Information Security Program Plan.

(8) Content and Format. The content and format for the NASA Automated Information Security Program Plan is shown in Exhibit 5-1.

EXHIBIT 5-1

| NASA AUTOMATED INFORMATION SECURITY PROGRAM PLAN FORMAT |
| --- |
| • MANAGEMENT SUMMARY<br>  - Background<br>  - History<br>• CURRENT SITUATION<br>• FUTURE STRATEGIES |

b. Program Office Computer Security Plan (PO-CSP)

(1) Program Offices are designated for agencywide programs. Many of these programs use computers and/or computer applications at NASA centers. PO-CSM's must ensure that HQ PO-CSP's address this use. PO-CSP's should be coordinated with appropriate center and DPI level CSP's to assure consistency.

(2) The PO-CSP should provide overall direction for computer security planning and adequate management summary information to support management oversight functions that assure appropriate security of all program office automated information resources. The content should be consistent with and provide input for the NASA Automated Information Security Program Plan. PO-CSP's may reference more detailed information found in other Program Office, center, or DPI plans. Actual computer security planning activities should be integrated into the more traditional planning activities, to the extent feasible, at Program Offices, centers, and DPI's.

(3) PO-CSP's should be updated annually and copies forwarded to the NASA Automated Information Security Program Manager by July 15.

## 502 CENTER COMPUTER SECURITY PLANNING

a. Center Computer Security Plan (CCSP)

(1) Scope. A computer security plan is needed for each NASA center.

(2) Purpose. The purpose of the CCSP is to summarize the status and direction of computer security activities throughout the center and at DPI's under the cognizance of the center. The intent is not to repeat details already documented in each DPI-CSP, but to integrate these plans into one consolidated document enabling DPI managers to plan for major computer security activities, to resolve inter-DPI conflicts and inconsistencies, and to provide overall computer security oversight and coordination at the center level.

(3) Manager. The CCSM is responsible for the development and maintenance of a computer security plan covering all automated information resources under the management or oversight of his or her center.

(4) Distribution. A copy of the CCSP should be sent to the NASA Automated Information Security Program Manager by July 15, but its primary use is for center managers.

(5) Publication Date. The CCSP shall be updated/revised annually and published by July 1.

(6) Period Covered. Computer security plans for NASA centers should comprehensively cover computer security activities over a 3-year period (prior year through current budget year plus one).

(7) Relationship with Other Plans. Center emergency response plans should reflect the security activities in the CCSP. The CCSP should incorporate, in summary form, information from all DPI-CSP's under the management or oversight of the center. In case of differences between a PO-CSP and a CCSP, the CCSP shall take precedence. If a PO-CSP requires more security than provided by the CCSP, the sponsoring PO shall be responsible for providing additional funding to meet such requirements. However, PO-CSP's must at least meet minimum baseline security requirements of a CCSP.

b. Content and Format. The level of detail in the CCSP is determined by the complexity and scope of the center's automated information resources. A sample format is shown in Exhibit 5-2.

(1) Introduction and Overview. The "Introduction and Overview" paragraph should define the Center Computer Security Program environmental context. This might include:

(a) Identifying those constraints that may impact the implementation of the overall Center Security Program.

(b) Describing the management structures, relationships, and personnel (DPI-CSO's, information owners and users, application sponsors, working groups, committees, etc.) that have responsibilities for the implementation and maintenance of the Center Computer Security Program.

(c) Describing the management processes established to ensure that DPI activities are carried out in a timely and complete fashion.

(2) Center Computer Security Program Goal and Objectives. The CCSP should have a paragraph clearly defining the Center Computer Security Program goal and objectives.

(3) Major Computer Security Activities

(a) The "Major Computer Security Activities" paragraph should describe all significant computer security activities over the 3-year period. Each activity could be related to the computer security goal and objectives defined earlier. For each year in the 3-year period, centers could cover specific activities with actual or anticipated completion dates.

(b) These activities should be consistent with those shown in the applicable DPI-CSP's. However, they would appear here in summary form only. Specific activities might include, but are not limited to:

(1) Risk Management.
(2) Application Certifications.
(3) Management Reviews.
(4) Computer Security Training.
(5) Personnel Screening.
(6) Network Security.
(7) Contractor Security.
(8) Major Incident Resolutions.
(9) Conferences.
(10) Reporting Problems.

## EXHIBIT 5-2
## CENTER COMPUTER SECURITY PLAN

1. EXECUTIVE SUMMARY

2. INTRODUCTION AND OVERVIEW

3. GOALS (NOTE: These are center-wide computer security program goals)

4. OBJECTIVES

5. COMPUTER SECURITY ACTIVITIES
   (NOTE: Each activity should list which computer security goals and objectives it supports.)

   a. Prior Year Accomplishments
   b. Current Budget Year Activities
   c. Current Budget Year Plus One Activities

6. COMPUTER SECURITY ACTIONS REQUIRING COORDINATION WITH OTHER CENTERS, NASA HEADQUARTERS, OR OTHER FEDERAL AGENCIES

7. OTHER COMMENTS

(c) Where possible, centers could identify the financial and personnel resources needed to support the computer security activities. These needs could include NASA personnel, contractual support, and personnel training. When funding is endemic to the development, operation, or maintenance of computer systems or automated applications, centers could estimate the percentage of that funding that is (or will be) directed toward computer security activities.

## 503 DPI COMPUTER SECURITY PLANNING

a. Purpose. The purpose of the DPI-CSP is to provide a document that serves as the management summary of more detailed information that may be associated with the basic elements of the DPI's computer security program. It should serve as a basis for informing management of security needs, performing security assessments, performing management and compliance reviews, and facilitating the extraction of summary information in response to center, HQ, or other Federal agency requests for planning information. The extent to which this planning activity is integrated into the center planning activities is left to the discretion of each CCSM; however, a DPI must comply with the center's CSP.

b. Content. The DPI-CSP must be kept current and should include elements that are relative to the coverage of the plan and to the computing environment of the DPI, as follows (see Exhibit 5-3):

(1) Summary of the management process describing the general administrative, technical, physical, and personnel protective measures employed at the DPI. If special provisions apply to selective computer systems or applications, this information should be included.

(2) Reference to list(s) that uniquely identify computer applications that process sensitive or mission-critical information, the sponsors and/or owners of such applications, and the computer systems that provide processing support.

EXHIBIT 5-3

**DPI COMPUTER SECURITY PLAN ELEMENTS**

- Current Controls
- Application Sensitivities
- Contingency Plans
- Actions Schedule
- Review Results
- Awareness & Training
- Security Tools
- Incident Identification
- Security Contacts

(3) Reference to contingency and disaster recovery plans.

(4) Reference to schedules indicating planned and completed risk assessments, certifications/recertifications, compliance reviews, and CSAT sessions. Schedules should, at a minimum, indicate the fiscal year planned for such tasks.

(5) Reference to documents containing the results of the latest compliance reviews, risk assessments, security design reviews, system tests, certifications/recertifications, and followup actions on previous recommendations from these review activities.

(6) Reference to a plan for continually providing CSAT to personnel who manage, design, develop, operate, maintain, or use computer systems. Plans for off-site users may be less specific and describe approaches for disseminating security awareness and training information (e.g., online tutorials and security bulletins).

(7) Identification of software tools used to enhance security.

(8) Reference to the procedures for identifying computer security incidents and reporting significant incidents.

(9) Reference to lists of key personnel and how they can be contacted during emergencies. Key personnel may include but are not limited to:

(a) The DPI-CSO.
(b) Assistant DPI-CSO's.
(c) CSC's.
(d) Computer security incident response personnel.

(1) DPI management.
(2) Operations.
(3) Technical support.
(4) Information sponsors/owners/users.

(e) Physical emergency response personnel.

(1) Building maintenance.
(2) Building protective services.
(3) Fire department.

## 504 DPI CONTINGENCY AND DISASTER RECOVERY PLANS

Contingency and Disaster Recovery Plans are covered in paragraph 308.

## 505 EXTERNAL REQUESTS FOR REPORTS ON PLANNING ACTIVITY

a. NASA is subject to ongoing requests for reports of computer security planning activity from such external agencies as OMB, NIST, NSA, GSA, and GAO. To reduce management burden and administrative paperwork, detailed documentation (related to the basic elements of computer security planning) should be maintained at the lowest organizational levels. This information should be stored in ways that make it easily located, extracted, analyzed, and formatted.

b. Exhibit 5-4 illustrates the relationship of all NASA computer security planning activities. The flow of planning information (from general requirements to specific security information) provides a master directory and cross-reference system for locating detailed documentation on any specific aspect of the agencywide CSP. This systematic approach eliminates the need to retain multiple copies of documents at DPI, center, and Headquarters levels. However, this structure requires that:

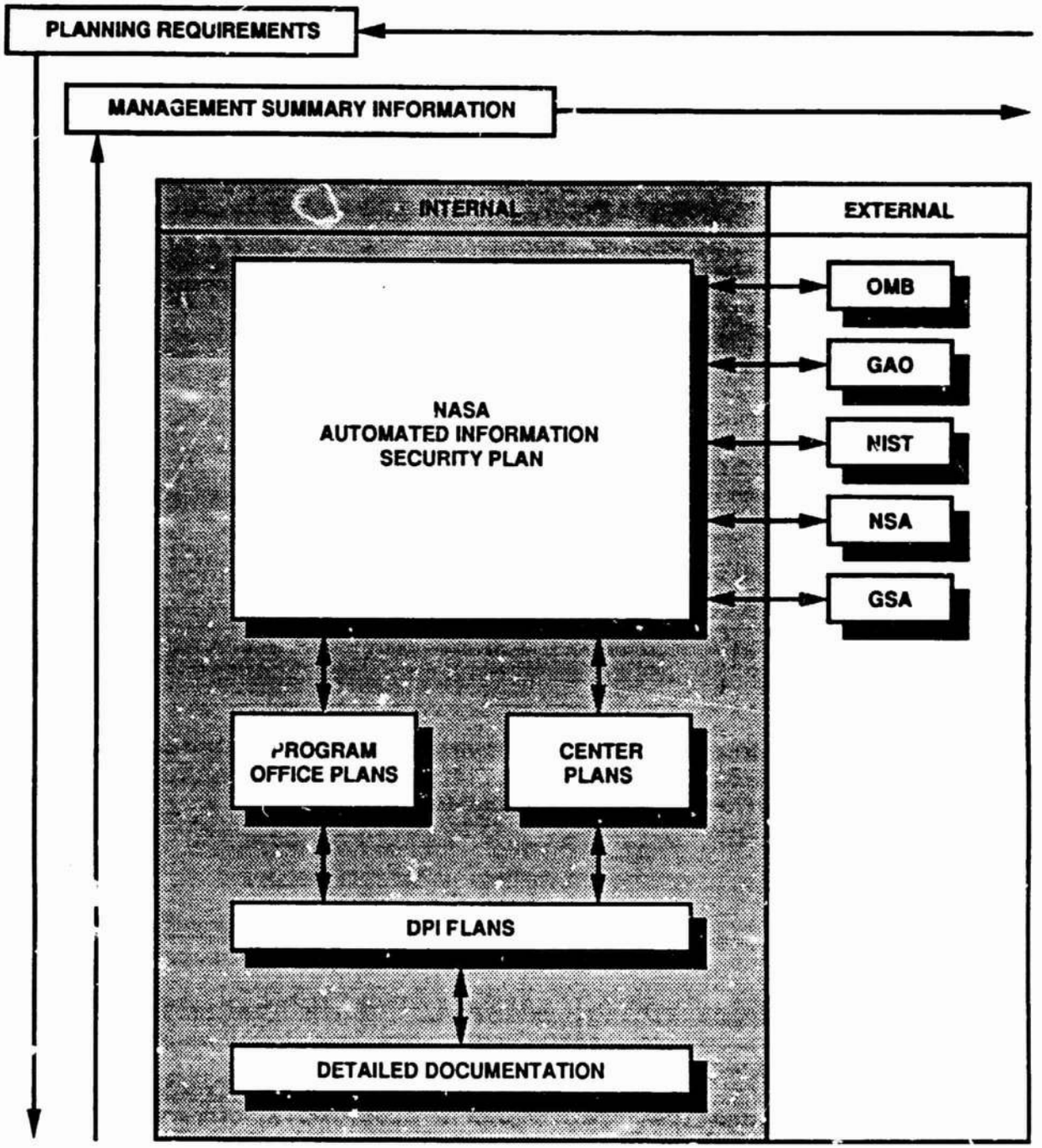
(1) The NASA Automated Information Security Program Plan references more detailed information contained in HQ Program Office and center computer security plans.

(2) The Program Office and center plans reference more detailed information contained in DPI-CSP.

(3) The DPI-CSP references more detailed information in computer system-level documentation.

c. An example of an external request is documented in OMB Bulletin 88-16, issued July 6, 1988. OMB Bulletin 88-16 required computer systems that processed sensitive information to be identified by drawing logical boundaries around major application support systems and/or general hardware support systems, based on the similarities among functional security requirements and options. NASA is able to comply with such requests using existing organizational structures (i.e., HQ Program Offices, centers, and DPI's) and consolidating information contained in existing documentation (at all levels).

**EXHIBIT 5-4**
**RELATIONSHIPS AMONG COMPUTER SECURITY PLANNING ACTIVITIES**



# CHAPTER 6. SPECIAL CONSIDERATIONS FOR MICROCOMPUTERS

## 600 INTRODUCTION

a. Security Principles. All the computer security policies, standards, responsibilities, guidelines, principles, and techniques covered in Chapters 1 through 5 apply to microcomputers. However, the application of those policies, standards, responsibilities, guidelines, principles, and techniques can vary dramatically.

b. Security Implications. Microcomputer characteristics result in security implications not normally found on mainframes:

(1) The increased use of microcomputers on networks has exposed them to external threats.

(2) Microcomputer operating systems have few, if any, security features designed into them.

(3) Most users do not understand the protective measures available for microcomputers.

(4) Microcomputers normally operate in office areas and are, therefore, accessible to most employees.

(5) Microcomputers are easy to move, and therefore can be easily stolen. In addition, moving a microcomputer can damage it internally.

(6) Most users do not understand that protective measures are necessary to safeguard the valuable data, and not just the loss of the computer hardware.

## 601 SPECIAL PROTECTIVE MEASURES FOR MICROCOMPUTERS

The following paragraphs identify security implications of microcomputers that require special protective measures.

a. Technical Protective Measures. The following technical protective measures for microcomputers are available as software or hardware add-ons:

(1) Sensitive information encryption.
(2) Computer access control using passwords.
(3) Erased disk area overwrite.

(4) Disk backup.
(5) Deleted files retrieval.
(6) Authorized program execution control.

b. Administrative Protective Measures. The following administrative protective measures are available for microcomputers:

(1) Virus-free microcomputer input verification.
(2) Licenses for all software purchased for use.

c. Physical Protective Measures. The following physical protective measures are available for microcomputers:

(1) Keyboard lock.
(2) Computer tie-down device.
(3) Diskette storage cabinet.
(4) Removable hard disk.
(5) Lockable office or enclosure.

d. Personnel Protective Measures. Personnel security for microcomputers might include:

(1) User Security Awareness and Training.
(2) Employee Screening and Monitoring.

## APPENDIX A. REFERENCES

A. FEDERAL DOCUMENTS


1. Executive Order 12356, "National Security Information," dated April 1982.

2. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," dated December 1985.

3. OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," dated July 1988.

4. Office of Personnel Management Regulation, "Training Requirement for the Computer Security Act," dated July 1988.

5. Title 41, Code of Federal Regulations, Chapter 201, Parts 201- 6 and 201-7, entitled "Protection of Personal Privacy," and "Security of Information Resource Systems," respectively.

6. National Bureau of Standards (now the National Institute for Standards and Technology) "Computer Security Training Guidelines," dated July 1988.

7. Federal Information Processing Standards Publication (FIPS PUB) 73, "Guidelines for Security of Computer Applications," dated June 1980.

8. FIPS PUB 39, "Glossary for Computer Systems Security," dated February 1976.

9. DOD Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, dated December 1985.

10. National Computer Security Center, NCSC-TG-004, Version 1, "Glossary of Computer Security Terms," dated October 1988.


B. NASA MANAGEMENT INSTRUCTIONS AND HANDBOOKS


1. NMI 1152.19, "NASA Information Security Program Committee."

2. NMI 1200.7, "NASA's Internal Control System."

3. NMI 1371.3, "Coordination of Foreign Visitor Activity."

4. NMI 1610.3, "Personnel Security Program."

5. NHB 1610.6, "NASA Personnel Security Handbook."

6. NMI 1630.2, "Delegation of Authority to Certify for Access to Restricted Data."

7. NHB 1640.4, "NASA Information Security Program."

8. NMI 1640.7, "Delegation of Authority to Make Determinations in Original Classification Matters."

9. NMI 1650.1, "Industrial Security Policies and Procedures."

10. NHB 2410.1, "Information Processing Resources Management."

11. NMI 2410.7, "Assuring the Security and Integrity of NASA Automated Information Resources."

12. NMI 2520.1, "Communications System Management."

13. NMI 9810.1, "The NASA Investigations Program."

C. NASA HEADQUARTERS IRM OFFICE DOCUMENTS

NASA Computer Security Awareness and Training (CSAT) Guide, dated April, 1990.

## APPENDIX B. ABBREVIATIONS

| Abbreviation | | Meaning |
|---|---|---|
| ADP | - | Automatic Data Processing |
| AIS | - | Automated Information System |
| AOSS | - | Automated Office Support Systems |
| ARC | - | Ames Research Center |
| CAI | - | Computer-Assisted Instruction |
| CCSM | - | (NASA) Center Computer Security Manager |
| CCSP | - | (Field) Center Computer Security Plan |
| COMSEC | - | Communications Security |
| CPU | - | Central Processing Unit |
| CRT | - | Cathode Ray Tube |
| CSAT | - | Computer Security Awareness and Training |
| CSC | - | Computer Security Coordinator |
| CSIR | - | Computer Security Incident Response |
| CSM | - | Computer Security Manager |
| CSP | - | Computer Security Plan |
| DAA | - | Designated Approving Authority |
| DBMS | - | Data Base Management System |
| DOC | - | Department of Commerce |
| DOE | - | Department of Energy |
| DOD | - | Department of Defense |
| DOJ | - | Department of Justice |
| DPI | - | Data Processing Installation |
| DPI-CSO | - | Data Processing Installation Computer Security Official |

| | | |
|---|---|---|
| DPI-CSP | - | Data Processing Installation Computer Security Plan |
| E.O. | - | Executive Order |
| FBI | - | Federal Bureau of Investigation |
| FIPS PUB | - | Federal Information Processing Standard Publication |
| FIRMR | - | Federal Information Resources Management Regulation |
| FY | - | Fiscal Year |
| GSA | - | General Services Administration |
| GSFC | - | Goddard Space Flight Center |
| HQ | - | Headquarters (NASA) |
| IDS | - | Intrusion Detection System |
| IRM | - | Information Resources Management |
| ITSP | - | Information Technology Systems Plan |
| LaRC | - | Langley Research Center |
| LCM | - | Life-Cycle Management |
| LeRC | - | Lewis Research Center |
| JPL | - | Jet Propulsion Laboratory |
| JSC | - | Lyndon B. Johnson Space Center |
| KSC | - | John F. Kennedy Space Center |
| MCSC | - | Microcomputer Security Coordinator |
| MSFC | - | George C. Marshall Space Flight Center |
| NASA | - | National Aeronautics and Space Administration |
| NCSC | - | National Computer Security Center |
| NHB | - | NASA Handbook |
| NIST | - | National Institute of Standards and Technology |
| NMI | - | NASA Management Instruction |

| | | |
|---|---|---|
| NTISSC | - | National Telecommunications and Information Systems Security Committee |
| NTISSI | - | National Telecommunications and Information Systems Security Instruction |
| NSA | - | National Security Agency |
| NSDD | - | National Security Decision Directive |
| OMB | - | Office of Management and Budget |
| OPM | - | Office of Personnel Management |
| OPSEC | - | Operations Security |
| PC | - | Personal Computer |
| PCL | - | Personnel (Security) Clearance |
| PDS | - | Protected Distribution System |
| PO-CSM | - | (NASA HQ) Program Office Computer Security Manager |
| PO-CSP | - | (NASA HQ) Program Office Computer Security Plan |
| SAISS | - | Subcommittee on Automated Information Systems Security (NTISSC) |
| SSC | - | John C. Stennis Space Center |
| U.S.C. | - | United States Code |

## APPENDIX C. DEFINITIONS

ACCEPTABLE RISK - A level of risk at which there is reasonable assurance of management acceptance. In practice, acceptability of risk is a judgement call, based on local details (e.g., security specifications, systems testing results, appropriateness and completeness of the requirements definitions, perceptions of the threat environments, and compliance with applicable policies).

ACCESS CONTROL - The process of limiting access to information or to resources of a computer system to authorized users.

ACCESS CONTROL MEASURES - Hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these designed to detect or prevent unauthorized access to a computer system and to enforce access control.

ACCOUNTABILITY - The property that enables activities on a computer system to be traced to individuals who can then be held responsible for their activities.

ACCOUNTABILITY INFORMATION - A set of records, often referred to as an audit trail, that provides documentary evidence of processing, or other actions related to the security of a computer system.

ACCREDITATION - The formal declaration by a designated official that an automated information system or network is approved to operate:

- In a particular security mode;
- With a prescribed set of technical and nontechnical security safeguards;
- Against a defined threat;
- In a given operational environment;
- Under a stated operational concept;
- With stated interconnections to other automatic information systems or networks; and
- At an acceptable level of risk for which the accrediting official has formally assumed responsibility.

The accreditation statement affixes security responsibility with the accrediting official and shows that appropriate care has been taken for security.

ADMINISTRATIVE SECURITY - The management procedures and constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for classified information.

APPLICATION - A set of commands, instructions, and procedures, usually in software, which cause a computer system to process information. To avoid confusion in this Handbook, the phrase "automated application" is normally used.

APPLICATION INTERNAL CONTROLS - Security controls in the application software. The objectives of these controls include information validation, user identity verification, user service authorization verification, journaling, variance detection, and encryption.

APPROPRIATE - Actions, policies, procedures, or events that are reasonably defensible, based on local environments, risk assessments, and generally accepted practices. Since the NASA Computer Security Program Manager does not and cannot prescribe sufficient and reasonable detailed procedures for all situations NASA-wide, local managers must make many decisions concerning the appropriateness of local actions, policies, procedures, and events. These decisions will be discussed during regular management reviews by NASA HQ personnel.

ASSURANCE TESTING - A process used to determine that the security features of a system are implemented as designed, and that they are adequate for the proposed environment. This process may include hands-on functional testing, penetration testing, and/or verification.

AUTHENTICATION - The act of verifying the claimed identity of an individual, station, or originator.

AUTHORIZATION - The privilege granted to an individual by a designated official to access information based upon the individual's clearance and need-to-know.

AUTOMATED INFORMATION - All recorded information regardless of its media form (e.g., audible tone; paper; magnetic core, tape, or disk; microform; electronic signal; and visual/screen displays) that is processed by or stored for the purpose of being processed by a computer system. The terms "automated information," "automated data,"

"information," and "data" are considered synonymous and used interchangeably in this Handbook.

AUTOMATED INFORMATION RESOURCES - Data and information; computers, ancillary equipment, software, firmware, and similar procedures; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

AUTOMATED OFFICE SUPPORT SYSTEMS (AOSS) - AOSS includes stand-alone microprocessors, word processors, memory typewriters, and terminals connected to mainframes.

AVAILABILITY - The state that exists when data can be obtained within an acceptable period of time.

CATEGORY - A grouping of information for which specific labelling and/or handling must be used and which should influence the choice of computer security controls. This Handbook lists 13 of these information categories.

CENTER - A major NASA site as defined in NMI 1101.2, "NASA Organization and Definition of Terms." The following are considered NASA centers:

- Ames Research Center (ARC)
- George C. Marshall Space Flight Center (MSFC)
- Goddard Space Flight Center (GSFC)
- John C. Stennis Space Center (SSC)
- John F. Kennedy Space Center (KSC)
- Langley Research Center (LaRC)
- Lewis Research Center (LeRC)
- Lyndon B. Johnson Space Center (JSC)
- NASA Headquarters (HQ)

CERTIFICATION - A written acknowledgement (by a NASA management official) that there is reasonable assurance that an automated application and its automated environment:

- Meet all applicable NASA and other Federal policies, regulations, and standards covering security; and

- Have been tested and technically evaluated thoroughly enough to demonstrate that the installed security controls are adequate.

Certification is based on applicable vulnerability analyses, risk analyses, management reviews, testing reports, etc. Certification is the final management decision point in the

quality control process which assures the automated application and the current operational environment (such as, hardware, operating systems, communications systems, and multiuser security packages) are sufficiently secure to support that automated application.

CLASSIFIED COMPUTER SECURITY PROGRAM - All of the technological safeguards and managerial procedures established and applied to computer facilities and computer systems (including computer hardware, software, and data) in order to ensure the protection of classified information.

CLASSIFIED DATA/CLASSIFIED INFORMATION - Top Secret, Secret, and/or Confidential information, regardless of category, for which NASA is responsible, and which requires safeguarding in the interest of national security.

CLEARING - The overwriting of information on magnetic media such that the media may be reused. (This does not change the classification level of the media.) For example, volatile memory can be "cleared" by removing power from the unit for a minimum of one minute.

COMMUNICATIONS SECURITY (COMSEC) - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

COMPLIANCE REVIEW - A review and examination of records, procedures, and review activities at a DPI in order to assess the computer security posture and ensure compliance with this Handbook. This review is normally conducted by the CCSM at a field center having cognizance over the DPI and having management responsibilities for implementing this Handbook.

COMPROMISE - The disclosure of classified data to persons who are not authorized to receive such data.

COMPROMISING EMANATIONS (TEMPEST) - Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, could disclose classified information being transmitted, received, handled, or otherwise processed by any information processing equipment.

COMPUTER FACILITY - One or more rooms, generally contiguous, containing the elements of a computer system.

COMPUTER SECURITY INCIDENT - An adverse event associated with a computer system that results in:

- A failure to comply with security regulations or directives;
- An attempted, suspected, or actual compromise of sensitive or classified information;
- The waste, fraud, abuse, loss, or damage of Government property or information; or
- The discovery of a vulnerability.

COMPUTER SYSTEM - A logical aggregation of automated information resources into a related set of processing capabilities performing one or a series of generally related tasks. For example, interconnected mainframe computers, served by front-end communications processors, maintained and operated under a specific contract, and associated peripheral input/output and storage devices, performing a number of administrative tasks could be considered a "computer system." A single minicomputer supporting a variety of graphics work stations and/or controlling experimental equipment could also be considered a "computer system." Included in this definition are word processors, microprocessors, personal computers, controllers, AOSS, memory typewriters, and other stand-alone or special computer systems.

CONFIDENTIALITY - The state that exists when data are held in confidence and are protected from unauthorized disclosure.

CONFIGURATION MANAGEMENT - Control of changes made to a computer system's hardware, software, and/or documentation (including an inventory of the system elements) throughout the development and operational life of the system.

CONTINGENCY PLAN - A document, developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations (including disasters). Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

CRITICAL RESOURCES - Those physical and information assets required for the performance of the installation's mission.

CRITICALITY RATING - An importance-related and/or time-related designation assigned to a computer application that

indicates when it must be back in operation to avoid mission impacts after a disaster or interruption in computer support services at a multiuser installation. To facilitate prioritized recovery procedures and for operating at offsite backup facilities in a degraded mode, computer applications should be assigned criticality ratings of varying importance (e.g., most critical, critical, important, deferrable). Applications with the same criticality rating should be additionally ranked (e.g., numerically) according to installation-determined processing priorities and perceptions of importance.

DATA PROCESSING INSTALLATION (DPI) - A logical grouping of one or more computer systems with common environmental and/or security characteristics for computer security management purposes.

DESTRUCTION - The physical alteration of computer system media or computer system components such that they can no longer be used for storage or retrieval of information.

DISASTER RECOVERY PLANS - Documents containing procedures for emergency response, extended backup operations, and post-disaster recovery should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objectives of these plans, in conjunction with contingency plans, are to provide reasonable assurance that a computer installation can recover from such incidents, continue to process mission-critical applications in a degraded mode and return to a normal mode of operation within a reasonable time. Such plans are a protective measure generally applied based on assessments of risk, cost, benefit, and feasibility and an evaluation of other protective measures in place.

EXCLUSION AREA - A security area for the protection of classified materials where mere access to the area would result in access to those classified materials.

INFORMATION - The terms "information," "data," "material," "documents," and "matter" are considered synonymous and used interchangeably in this Handbook. They refer to all data regardless of its physical form (e.g., data on paper printouts, tapes, disks or disk packs, in memory chips, in Random Access Memory (RAM), in Read Only Memory (ROM), on microfilm or microfiche, on communication lines, and on display terminals).

INFORMATION RESOURCES MANAGEMENT (IRM) - The planning, budgeting, organizing, directing, training, and control of information and related resources (such as personnel, equipment, funds, and technology).

INSTALLATION SECURITY OFFICER - The designated Security Officers at a NASA Center who are responsible for the center's personnel, physical, information, industrial, and operations security programs.

INTEGRITY - The state that exists when computerized data are the same as those in the source documents or have been correctly computed from source data and have not been exposed to accidental or malicious alteration or destruction.

INTELLIGENCE INFORMATION - Classified information defined as intelligence information by Director of Central Intelligence Directive 1/19.

LABEL - The marking of an item of information to reflect its information category and/or security classification. An internal label is contained within the confines of the medium containing the information and reflects the classification and sensitivity of that information. An external label is a visible and readable marking on the outside of the medium (or the cover of the medium) that reflects the category and/or classification of the information within the medium.

LIMITED AREA - A security area for the protection of classified matter where guards, security inspectors, or other internal controls can prevent access.

LONG-RANGE PLAN - A written description of the strategy for implementing a program covering the next 5 years.

MULTILEVEL SYSTEMS - Systems/networks that incorporate the mode of operation that allows two or more classification levels (including unclassified) of information to be processed simultaneously within the same system when some users are not cleared for all levels of information present.

MANAGEMENT REVIEW - A review and examination of records, activities, policies, and procedures established by field centers to manage and coordinate computer security programs under their cognizance. This review is normally conducted by Headquarters personnel with NASA-wide computer security program management responsibilities.

MISSION-CRITICAL INFORMATION - Plain text or machine-encoded data that, as determined by competent authority (e.g., information owners), have high importance related to accomplishing a NASA mission and require special protection because unnecessary delays in processing could adversely affect the ability of NASA, an owner organization, or a NASA center to accomplish such missions.

NETWORK - A communications medium and all components attached to that medium that are responsible for the transfer of information. Such components may include computer systems, packet switches, telecommunications controllers, key distribution centers, technical control devices, and other networks.

NON-FEDERAL PERSONNEL - Non-civil servant employees. The use of the term non-Federal personnel in paragraph 306 of this Handbook does not include foreign nationals.

OPERATIONS SECURITY (OPSEC) - OPSEC is the process of denying adversaries information about friendly intentions, capabilities, plans and programs by identifying, controlling and protecting intelligence information and indicators associated with planning and conducting military operations as well as other defense activities not already afforded adequate protection as classified information.

PASSWORD - A protected word, phrase, or a string of symbols that is used to authenticate the identity of a user.

PASSWORD SPACE - The total number of possible passwords that can be created by a given password generation scheme.

PERSONNEL SCREENING - A protective measure applied to determine that an individual's access to sensitive information is admissible. The need for and extent of the screening process is normally based on an assessment of risk, cost, benefit, and feasibility, as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual.

PERSONNEL SECURITY - The procedures established to ensure that all personnel who have access to classified information have the required authorization, as well as the appropriate clearances.

PHYSICAL SECURITY - The use of locks, guards, badges, alarms, procedures, and similar measures (alone or in combination)

to control access to a computer system and related equipment, and structures from espionage, theft, waste, fraud, abuse, or damage by accident, fire, and environmental hazards.

PROGRAM OFFICE (HEADQUARTERS) - A focal point within NASA HQ (such as Codes M, O, R, and S) with management control responsibility for research and development activity within their functional area at NASA field centers.

PROPERTY PROTECTION AREA - An area set aside for the protection of property, as required by this Handbook.

PROTECT AS RESTRICTED DATA (PARD) - A handling method for computer-generated numerical data, or related information, which is not readily recognized as classified or unclassified because of the high volume of output and low density of potentially classified data. Information is designated as PARD because it has not had a sensitivity (classification) review and must be protected under a different set of security rules.

PROTECTED DISTRIBUTION SYSTEM (PDS) - A telecommunications system to which acoustical, electrical, electromagnetic, and physical safeguards have been applied to permit its use for secure electrical or optical transmission of unencrypted classified information or sensitive unclassified information.

PROTECTION INDEX - A measure of perceived risk determined from the combination of the clearance level of users and the classification of the data on the classified computer system. The determination of this index is described in Chapter 8.

PROTECTION MEASURES - Physical, administrative, personnel, and technical security measures that, when applied separately or in combination, are designed to reduce the probability of harm, loss, damage to, or compromise of, a computer system or automated information.

QUALITATIVE RISK ASSESSMENT - A risk assessment that uses labels (such as, high, medium, and low), rather than actual numbers, to characterize anticipated likelihood and extent of harm to automated information resources.

QUANTITATIVE RISK ASSESSMENT - A risk assessment that requires the use of actual numbers, calculations of Annual Loss Expectancy (ALE), and mathematical probabilities to characterize the anticipated likelihood and extent of harm to automated information resources.

RECERTIFICATION - An ongoing assurance that a previously certified system has been periodically reviewed, that compliance with established protection policies and procedures remains in effect, and that security risks remain at an acceptable level.

RISK ASSESSMENT - An identification of a specific computer facility's assets, the threats to these assets, and the computer facility's vulnerability to those threats. Risk assessment is a management tool that provides a systematic approach for:

- Determining the relative value and sensitivity of computer installation assets;
- Assessing vulnerabilities;
- Assessing loss expectancy or perceived risk exposure levels;
- Assessing existing protection features and additional protection alternatives or acceptance of risk; and
- Documenting management decisions.

Decisions for implementing additional protection features are normally based on the existence of a reasonable ratio between cost/benefit of the safeguard and sensitivity/value of the assets to be protected. Risk assessments may vary from an informal review of a small-scale microcomputer installation to a more formal and fully-documented analysis (i.e, risk analysis) of a large-scale computer installation. Risk assessment methodologies may vary from qualitative or quantitative approaches to any combination of these two approaches.

SANITIZATION - The elimination of classified information from a computer system or media associated with a computer system to permit the reuse of the computer system or media at a lower classification level, or to permit the release to uncleared personnel or personnel without the proper information access authorizations.

SECURITY AREA - A physically defined space containing classified matter (documents or material) subject to physical protection and personnel access controls.

SECURITY DESIGN REVIEW - A review process in which the objective is to ascertain whether implemented protective measures meet the original system design and approved computer application

security requirements. The security design review may be a separate activity or an integral function of the overall application system design review activity.

SENSITIVE ADP POSITION - A personnel position that cannot be occupied until completion of an employee background check.

SENSITIVE INFORMATION - Plain text or machine-encoded data that, as determined by competent authority (e.g., information owners), have relative sensitivity and require mandatory protection because of statutory or regulatory restrictions (e.g., "for official use only" information, information subject to the Privacy Act of 1974, etc.) or require a degree of discretionary protection because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect National or other NASA interests (e.g., program- critical information or controlled scientific and technical information, which may include computer codes (computer programs) used to process such information).

SENSITIVITY AND/OR CRITICALITY LEVELS - Four NASA hierarchical groupings (labeled 0 through 3) used to help determine which computer security controls are needed.

SHORT-RANGE PLAN - A 1-year (i.e., tactical) plan.

SIGNIFICANT CHANGE - A change in a computer installation that could impact overall processing requirements and conditions or installation security requirements (e.g., adding a local area network; changing from batch to online processing; adding dial-up capability; carrying out major hardware configuration upgrades; operating system changes; making major changes to the physical installation; or changing installation location).

SIGNIFICANT COMPUTER SECURITY INCIDENT - An event that would be of concern to senior NASA management due to potential for public interest or embarrassment to the organization, or potential for occurrence at other NASA sites. These events may include: unauthorized access, theft, an interruption to computer service or protective controls, an incident involving damage, a disaster, or discovery of a vulnerability.

SPONSOR/OWNER - The local management individual with overall responsibility for the functional area supported by the an automated application. The sponsor/owner is the person responsible for development of functional security requirements.

SYSTEM DESIGNER - The person who interprets the functional security requirements (developed by the application sponsor/owner) and designs the technical security specifications.

SYSTEM DEVELOPER - The person who incorporates the technical security specifications into an operational system.

TECHNICAL FEASIBILITY ANALYSIS - A study to determine alternative controls for reducing identified risks.

TELECOMMUNICATIONS SECURITY - The domain of computer security that is concerned with protecting the point-to-point communication (e.g., input device to computer, computer to computer, etc.) of sensitive unclassified information with appropriate cost-effective measures (e.g., data encryption and protected distribution systems). Such communications generally occur via data communication systems, links, and devices such as wide area networks, local area networks, telephone/wire lines, fiber optics, radio waves/microwaves, and integrated circuits.

TEMPEST - A code name referring to the investigation and study of compromising emanations. It is sometimes used synonymously with the term "compromising emanations" (e.g., TEMPEST tests and TEMPEST inspections).

TRUSTED COMPUTER SYSTEM - A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of classified information.

USER - Any individual who can operate any equipment, implement a procedure that can access the computer system, input commands to the computer system, or receive output from the computer system without intervention of an authorized reviewing official. Note that a user may not necessarily be an authorized user of a computer system.

VERIFIABLE IDENTIFICATION FORWARDING - An identification method used in networks that allows the sending host to verify that an authorized user on its system is attempting a connection to another host. The sending host transmits the required user authentication information to the receiving host. The receiving host can then verify that the user is validated for access to its system. This operation may be transparent to the user.

## APPENDIX D. LIST OF EXHIBITS


| Number | Title | Page |
|---|---|---|
| 1-1 | National Policy and Guidance | 1-8 |
| 2-1 | NASA Automated Information Security Program Logo | 2-4 |
| 2-2 | Computer Security's Relationships With Other Security Disciplines | 2-7 |
| 2-3 | Headquarters Roles and Responsibilities | 2-8 |
| 2-4 | Who Is Responsible for Automated Information Security? | 2-11 |
| 2-5 | NASA Automated Information Security Program Structure (Part 1) | 2-13 |
| 3-1 | NASA Automated Information Security Program Structure (Part 2) | 3-3 |
| 3-2 | DPI-CSO Responsibilities | 3-4 |
| 3-3 | Management Process | 3-6 |
| 3-4 | Risk Assessment Steps | 3-8 |
| 3-5 | Recommended Protective Measures | 3-10 |
| 3-6 | Certifying New/Modified Applications | 3-11 |
| 3-7 | Screening Levels for Non-Federal Employees Working With Computers | 3-15 |
| 3-8 | Minimum Information for Foreign National Access Requests | 3-17 |
| 3-9 | Minimum Information for Follow-On Incident Report Content | 3-22 |
| 4-1 | NASA Automated Information Categories | 4-2 |
| 4-2 | NASA Unclassified Automated Information Sensitivity/Criticality Levels | 4-3 |

| Number | Title | Page |
|---|---|---|
| 4-3 | Protective Measure Considerations (Part I) | 4-5 |
| 4-3 | Protective Measure Considerations (Part II) | 4-6 |
| 4-4 | Categories and Sensitivities | 4-9 |
| 5-1 | NASA Automated Information Security Program Plan Format | 5-2 |
| 5-2 | Center Computer Security Plan | 5-5 |
| 5-3 | DPI Computer Security Plan Elements | 5-6 |
| 5-4 | Relationships Among Computer Security Planning Activities | 5-9 |
| 8-1 | Incident Ranking Table | 8-6 |
| 8-2 | Initial Incident Reporting Procedures | 8-7 |
| 8-3 | Accreditation Process for Systems Processing NASA Classified Information | 8-9 |

## APPENDIX E. CLASSIFIED SYSTEM SECURITY PLAN

A classified system security plan is prepared as the basic system security document and as evidence that the proposed classified computer system, or update to an existing classified computer system, meets the appropriate computer security program requirements for classified processing. The plan is used throughout the certification and accreditation process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. It also serves as the basis for inspections of classified systems. The CCSM shall maintain a current copy of all approved system security plans for the installation. The DAA shall maintain current accreditation documentation of systems for which they are the designated approving authority (i.e., accrediting official).

Note: A classified system security plan may contain classified information and shall be marked and protected according to NASA's established policies and procedures for classified handling.

1. ATTACHED DOCUMENTS. Where sections of the following information are common to several classified computer systems at an installation, the information may be contained in a separate document and that document attached to or referenced in each system security plan.

2. CLASSIFIED SYSTEM SECURITY PLAN CONTENTS. The plan formally documents the operation of a classified system and the mechanisms that are used to control access and protect the system and its information. To make appropriate accreditation decisions, the DAA needs to understand the complete system environment. Therefore, at a minimum, each plan shall contain the following information:

a. The identification and location of the computer system.

b. The name, location, and phone number of the responsible CCSM or DPI-CSO.

c. A narrative description of the classified computer system and the rules for permitting and denying access to the information that is processed, stored, transferred, or accessed by the system. These rules must describe how access will be controlled based on the classification of information processed, and the clearance level and need-to-know of users.

d. A description of the system's computing environment that includes at least:

(1) Determination of the protection requirements for the system.

(2) Description of the methods used to meet the above protection requirements including a description of security related software.

(3) The level and amount of classified information to be processed, stored, transferred, or accessed in the system.

(4) The architecture of the system, including all hardware components, showing the organization, interconnections, and interfaces of these components. (A schematic drawing may be used to satisfy this requirement.)

(5) A detailed inventory of the classified system components including software and hardware.

(6) Description of the control mechanisms to be used for review and approval of modifications to the classified system.

e. The evidence, or basis for certification, that each of the requirements of this Handbook have been met. This description shall specifically address the requirements of at least the following areas:

(1) Personnel Security.
(2) Physical Security.
(3) Telecommunications Security.
(4) Hardware and Software Security.
(5) Administrative Security.

f. A description of the management controls established to prevent waste, fraud, and abuse.

g. A risk assessment that provides a measure of the relative vulnerabilities and threats.

h. A description of the security training required for the personnel associated with the classified computing system.

i. The procedures to be used by the personnel associated with the classified system for reporting any computer security incidents to appropriate management. These procedures shall include the actions to be taken to secure the classified system during a security-related incident.

j. The contingency plan and recovery procedures for the classified system, including the designation of persons responsible for carrying out particular procedures, and the plan for testing the operations of the contingency plan.

k. A description of the process used to protect the current backup copies of critical software, information, and documentation.

l. Escort procedures, including procedures unique to this classified system.

m. A description of the controls for access to the classified system. If passwords are used for access control, describe how they are selected, their length, the size of the password space, etc.

n. The procedures for operating the system in an interim period during updates or changes to the system.

o. If remote diagnostic services are to be used, specify the methods of connection and disconnection and related security measures.