

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1

Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| [TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) |
[Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) |
[Chapter10](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#)
| [AppendixF](#) | [AppendixG](#) | [AppendixH](#) | [AppendixI](#) | [AppendixJ](#) |
[AppendixK](#) | [AppendixL](#) | [AppendixM](#) | [AppendixN](#) | [AppendixO](#) | [ALL](#) |

Chapter 8: Program Security

8.1 General

8.1.1. This chapter provides the requirements for establishing a system security approach in the development of a NASA program or in enhancing the protection level of an active program.

8.1.2. The objective is to identify security provisions as early as possible in system designs, acquisitions, or modifications, thereby minimizing costs, vulnerabilities, and compromises.

8.2 Responsibilities

8.2.1. The CCS for each Center is responsible for the following:

8.2.1.1. Establishing a system that ensures security requirements and provisions are identified at the outset of new or changing programs, acquisitions, and modifications.

8.2.1.2. Incorporating appropriate security measures, outlined in the various Chapters of this NPR, into project plans, facility plans, and requests for proposals.

8.2.2. Project and program managers at NASA Centers are responsible for ensuring provisions contained in Chapter 4, section 4.7 of NPR 7120.5B, NASA Program Project Management Processes and Requirements, are appropriately addressed with the CCS.

8.2.3. The DSMD shall compile and maintain the Agency Mission Essential Infrastructure (MEI) Inventory of NASA mission essential infrastructure assets. The List shall consist of:

8.2.3.1. Critical or Key Asset description (Cyber, Physical or both).

8.2.3.2. Owing Center/Program

8.2.3.3. Physical Location

8.2.3.4. Responsible Enterprise

8.2.3.5. Whether part of Agency Continuity Of Operations (COOP) Planning Program.

8.2.4. Center program/project managers shall ensure that critical programs or assets are identified for inclusion on the consolidated inventory and that program planning includes security provisions and funding.

8.3 Acquisition Systems Protection (ASP)

8.3.1. ASP enables the establishment of definitive security requirements in the acquisition or modification of systems, equipment, and facilities; the analysis of security design and engineering vulnerabilities; and the development of recommendations consistent with other design and operational considerations.

8.3.2. ASP supports the development of programs and standards that provide life-cycle security for critical NASA resources.

8.3.3. ASP establishes, as part of each major acquisition development and upgrade program, appropriate procedures to identify security risks and actions to eliminate or minimize associated vulnerabilities.

8.3.4. ASP provides a means to ensure that necessary security requirements (physical, personnel, technical, communications, and information) are adequately considered and, when appropriate, incorporated into the overall system development program.

8.3.5. The ASP plan for each Center shall incorporate security into major systems, as applicable, to support economical achievement of overall program objectives.

8.3.6. The plan shall include those security tasks applicable to each phase of the acquisition process.

8.4 NASA Critical Infrastructure and Key Resources -Mission Essential Infrastructure (MEI) Protection Program

8.4.1. Homeland Security Presidential Directive (HSPD) 7 "Critical Infrastructure Identification, Prioritization, and Protection," directs every Government agency to establish a program to identify critical essential infrastructure and key resources, evaluate these assets for vulnerabilities, and fund and implement appropriate security enhancements (procedural and physical) to mitigate vulnerabilities. NASA has elected to designate its critical infrastructure and key resources as MEI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

8.4.2. An effective critical asset protection program provides affordable, practical, and responsible protection, within acceptable risks, to those vital NASA resources that cannot reasonably be replaced or that have unique capabilities to support NASA goals.

8.4.3. Designated MEI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate security vulnerability risk assessment.

8.4.4. NASA MEI may include IT resources managed under the "Special Management Attention (SMA)" designator; critical components; communication, command, and control capability; Government-owned flight or experimental flight vehicles, shuttles, international space station and apparatus; and one-of-a-kind irreplaceable facilities.

8.4.5. Supporting infrastructure called "interdependencies" shall not be designated as MEI.

- a. "Interdependencies" includes those external and internal commercial elements that the Center MEI depend on to operate; e.g., electrical power, gas, communications

hubs, local area networks, telephone systems, etc.

- b. "Interdependencies" must nevertheless be evaluated for their vulnerability and assessed for their impact if lost, especially if they are "single points of failure." Vulnerability mitigation activity regarding NASA assets designated as "interdependencies" must also take the "single point of failure" aspect into account when developing their mitigation plans.

8.4.6. The NASA Mission Essential Infrastructure Protection Program (MEIPP) shall replace the NASA Resource Program (NRP). All existing NRP assets must be reevaluated against MEI criteria to determine if they warrant continued designation as a critical NASA asset under the MEI designation.

8.4.7. Policy and procedures shall be developed and implemented at each Center that accurately reflect Agency requirements for assessing MEI as outlined in this and other Agencywide requirements. This ensures Agencywide uniformity and consistency in the approach to performing the appropriate risk vulnerability risk assessments for each identified MEI.

8.4.8. Criteria and procedures NASA Centers shall use in identifying NASA's MEI are contained in Appendix H, Identifying and Nominating NASA Assets for the MEIPP.

8.4.9. Minimum security requirements for MEI facilities or facilities housing MEI assets are provided in Chapter 7, paragraph 7.7.4.

8.5 Operations Security (OPSEC)

8.5.1. National Security Decision Directive (NSDD) 298 establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program.

8.5.2. Security programs and procedures already exist to protect classified information. However, items of information generally available to the public and certain detectable activities can reveal the existence of and possible details regarding classified or sensitive information. Such indicators could potentially benefit those seeking to neutralize or exploit U.S. actions in areas of National security.

8.5.3. OPSEC is a systematic and proven process through which the Government and its supporting contractors can promote operational effectiveness. The process can deny potential adversaries information by identifying, controlling, and protecting generally unclassified evidence concerning the planning and execution of sensitive activities.

8.5.4. Agencies with minimal activities affecting National security are not required to establish a formal OPSEC program; therefore, NASA does not require a formal Agency-level OPSEC program, although some Centers have programs that do require OPSEC application.

8.5.5. The NASA minimum security standard is to employ OPSEC measures on all classified programs.

8.5.6. If OPSEC planning is warranted, program and project managers, in coordination with the Center Counterintelligence (CI) Office, shall develop and implement a project OPSEC plan that shall identify critical information or activity, analyze threat and vulnerability, assess risk, and apply appropriate countermeasures.

8.6 Risk Management Process

8.6.1. NASA has adopted a Risk Management approach in which the risk of loss must be weighed against the cost and operational impact of implementing established minimum-security standards.

8.6.2. Risk management provides a mechanism that allows security and program/project managers to recommend waivers to security standards based upon a threat assessment

and the determined risk to an asset.

8.6.3. Risk management is an integrated process of assessing the threat, vulnerabilities, and value of the resource and then applying appropriate safeguards and/or recommending the assumption of risk.

8.6.4. The CCS shall ensure that security standards, established in this and other NPR, are met or that appropriate requests for waivers are submitted and approved by the AA/OSPP.

8.6.4.1. Each Center Director (or for Headquarters, the Director for Headquarters Operations) is designated as the Risk Acceptance Authority (RAA) for the Center.

8.6.4.2. The RAA shall make the final determination on requests for waivers to security standards when the CCS has determined that the waiver shall pose a serious risk on the program.

8.7 Special Access Programs

8.7.1. A Special Access Program shall be created within NASA only upon specific written approval of the Administrator, and coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure required security protocols are implemented and maintained. .

8.7.2. All personnel security requirements for NASA personnel to establish and participate in Special Access Programs external to NASA must be coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure accountability of NASA equities..

8.7.3. All NASA security activity associated with Special Access Programs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG).

8.8. Secure Compartmented Information (SCI) Programs

8.8.1. SCI Programs shall only be created within NASA upon specific written approval of the Administrator and coordinated with the Chief, Intelligence Liaison and Special Access Programs Support Division to ensure required security protocols are implemented and maintained.

8.8.2. All requests for NASA personnel, including NASA contractors, to participate in SCI Programs external to NASA must be coordinated with the Chief, Intelligence and Special Access Programs Support Division to ensure accountability of NASA equities.

8.8.3. Failure to comply with the requirements of this section may result in denial of security clearance and suspension of SCI activity.

8.9 NASA Security Education and Training, and Awareness (SETA) Program

8.9.1. General.

8.9.1.1. The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them.

8.9.1.2. Management and employee involvement is essential to an effective security program.

8.9.1.3. An integral part of the overall NASA Security Program relies on the education and training of individuals regarding their security responsibilities.

8.9.2. Responsibilities.

8.9.2.1. As a minimum, the Center Director shall ensure that adequate procedures are in place whereby all NASA employees and contractor personnel, regardless of clearance

status, are briefed annually regarding Center security program responsibilities.

8.9.2.2. The CCS for each Center shall ensure that appropriate and knowledgeable security personnel provide and receive the applicable types of briefings or training as described in paragraph 8.8.3. below.

8.9.2.3. NASA supervisors shall ensure job-related, facility-oriented security education, and awareness instruction or training for newly assigned personnel are timely and properly coordinated with the CCS.

8.9.3. Required Briefings and Training.

8.9.3.1. Initial orientation briefings are given by security personnel (i.e., NASA and/or security services contractor) to acquaint new employees with local security procedures and employee responsibilities to protect personnel and Government property from theft, loss, or damage.

8.9.3.2. Initial orientation briefings must be conducted within 20 days of the new employee/contractor arrival.

8.9.3.3. Security orientation briefings are given by the responsible supervisor or designee to each new employee and shall include all security requirements and procedures for which the employee is to be specifically responsible.

8.9.3.4. Upon conclusion, the supervisor or designee must ensure that NASA Form 838, Employee Security Orientation/Indoctrination Record, is completed by both individuals.

8.9.3.5. The supervisor shall ensure that the record copy of the form is promptly forwarded to the CCS for processing and permanent filing.

8.9.3.6. The CCS shall ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance.

- a. This briefing shall include general security aspects affecting employment and a summary of restrictions and obligations associated with access to classified information that are imposed by statute or executive order. The briefing shall also include standards of behavior expected of persons in sensitive positions and the responsibility of security clearance holders to report behavior that shall disqualify an individual from security clearance eligibility.
- b. The security person giving the briefing shall ensure that the employee is made aware of the most current executive order number if the briefing form has not been revised to reflect that change.
- c. Upon conclusion of the briefing, a Standard Form 312, Classified Information Nondisclosure Agreement, is signed by both individuals (employee and person giving the briefing).
- d. Annual briefings are required for all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Clearances may be suspended or revoke for failure to attend annual training.

8.9.3.7. Classified custodians and any other custodians responsible for CNSI safes, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

8.9.3.8. Security personnel shall give other special security training or briefings to employees, as appropriate, related to SAP's, SCI, MEI, and the Mission Critical Space Systems Personnel Reliability Program.

8.9.3.9. Security personnel shall conduct foreign travel briefings to NASA travelers to enhance their awareness of potential hostile intelligence, terrorist, and criminal threats in the countries to which they are traveling. These briefings must also provide defensive measures and other practical advice concerning safety measures.

8.9.3.10. Security personnel shall conduct security termination briefings to employees whose personnel security clearances are being terminated due to termination of employment, transfer to another Center, or other reasons. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their responsibilities and penalties for unauthorized disclosure of CNSI even after termination of the clearance or employment.

8.10. Self-Inspections

8.10.1. This section sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the Information, Industrial, Personnel, Physical and Program Security at all NASA Centers.

8.10.2 The objective is to ensure that each Center is implementing their security program in accordance with all applicable NASA and Federal regulations and to identify areas that need to be addressed that are not in compliance with appropriate rules and regulations. The review will also pinpoint commendable areas of each security operation and identify areas that need additional support to complete their mission.

8.10.3 Responsibilities.

8.10.1.1. The Director, Security Management Division (DSMD) is responsible for the agency's self-inspection. The DSMD shall designate agency personnel to assist in carrying out this responsibility. The DSMD shall determine the means and methods for the conduct of self-inspections. These may include:

- (a) A review of relevant security directives, guides, training material and instructions
- (b) Interview with security representatives and customers
- (c) Review of Information, Industrial, Personnel and Physical Security Programs
- (d) Review of various files and documents pertaining to day to day operations

8.10.1.2. The DSMD shall develop a standard self-inspection guide/checklist to be used by the inspectors conducting the review. Each Center shall be inspected at least every 2 years. The format for documenting findings shall be set by the DSMD. The DSMD, in its oversight capacity, may schedule inspections of Centers on an as needed basis.

8.10.4. Coverage of Inspections

These standards are not all-inclusive. Each inspection may be adjusted to meet the coverage of the security programs in place at that particular center.

8.10.4.1. Personnel Security Coverage

- a. Personnel Security Program Oversight
- b. Basic Principles of Personnel Security Clearance Management
- c. Processing Personnel Security Clearance Request
- d. Coding of Position Sensitivity Level Designations for National Security Positions
- e. Temporary/Interim Access to CNSI
- f. Access to CNSI by Non-U.S.Citizens
- g. Acceptance of Prior Investigations and Favorable Personnel Security Clearance Determinations from Other Government Agencies and Organizations.
- h. Guiding Principles for Adjudication, Suspension, Denial or Revocation of Personnel Security Clearances
- i. Database, File, and recordkeeping management.
- j. Suitability Investigations and Determinations
- k. Review of Questionnaires for Suitability Investigations.
- l. Reinvestigation Requirements
- m. Designation of Security Risk Levels for Civil Servants and Contractors
- n. Personnel Security Investigative Processing Requirements for Non-NASA employees.
- o. Adjudication Process for Center, Facility, and IT System Access.

8.10.4.2. Information Security Coverage

- a. Original and Declassification Management
- b. Classifying, Marking, and Declassifying Classified National Security Information (CNSI) and Foreign Government Information (FGI)

- c. Access to CNSI and FGI
- d. Accountability and Control of CNSI and FGI
- e. Storage of CNSI and FGI
- f. Reproduction of CNSI and FGI
- g. Transmission of CNSI and FGI
- h. Release of Classified Information to Foreign Governments
- i. Destruction of CNSI and FGI
- j. Security Violations and Compromise of CNSI and FGI
- k. CNSI and FGI Meetings and Symposia
- l. Security Container, Vault, and Strong Room Management
- m. Access, Storage, Reproduction, Transmission, Destruction and Release of Sensitive But Unclassified Information (SBU).
- n. Agency Information Security Program Data Report, SF-311
- o. Security Classification Reviews for NASA Programs and Projects
- p. Security Education, Training and Awareness Program

8.10.4.3. Industrial Security Program

- a. Department of Defense Support Review
- b. Processing of DD Form 254
- c. Classified Security Contract Management
- d. Suspension, Revocation, and Denial of Access to Classified Information

8.10.4.4. Physical Security Program

- a. Security Control at NASA Centers
- b. NASA Photo Identification Badge Program
- c. NASA Photo -ID Issuance Criteria
- d. Inspection of Persons and Property
- e. Security Areas
- f. Facility Security
- g. Airfield and Aircraft Security
- h. Control and Issuance of Arms, Ammunition, and Explosives (AA&E)
- i. Standards for Secure Facilities and Conference Rooms
- j. Threat Management
- k. Security Force Procedure Review
- l. Review of Incident and Threat Report
- m. NASA Security Office Special Agent Badge and Credentials Review
- n. TSCM Procedures
- o. Threat Condition (THREATCONS) Program

8.10.4.5. Program Security

- a. Acquisition Systems Protection Review
- b. Review of NASA Critical Infrastructure and Key Resources - Mission Essential Infrastructure (MEI) Protection Program.
- c. Operations Security Review
- d. Risk Management Review
- e. Special Access Program Review
- f. NASA Security Program Education, Training and Awareness review

| [TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) |
[Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) |
[Chapter10](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) |
[AppendixE](#) | [AppendixF](#) | [AppendixG](#) | [AppendixH](#) | [AppendixI](#) |
[AppendixJ](#) | [AppendixK](#) | [AppendixL](#) | [AppendixM](#) | [AppendixN](#) |
[AppendixO](#) | [ALL](#) |

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#)

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
