

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



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1A

Effective Date: August 12,
2013

Expiration Date: August 12,
2018

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

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements

Responsible Office: Office of Protective Services

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [AppendixA](#)
| [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [AppendixF](#) | [AppendixG](#) | [AppendixH](#) | [ALL](#)

Chapter 3. Program Security and NASA Critical Infrastructure (NCI)

3.1 General

3.1.1 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.

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

3.2 Responsibilities

3.2.1 The CCPS/CCS for each Center is responsible for the following:

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

3.2.1.2 Incorporating appropriate security measures, outlined in the various chapters of this NPR and others, into project plans, facility plans, construction and modernization projects, and requests for proposals impacting program security.

3.2.2 Project and program managers at NASA Centers are responsible for ensuring provisions contained in NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, are appropriately addressed with the CCPS/CCS.

3.2.3 The AA, OPS shall compile and maintain the NCI inventory of NASA mission-essential infrastructure assets. The AA, OPS will identify critical infrastructure where a cyber-security incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The list will consist of:

- a. The critical or key asset description (cyber, physical, or both).
- b. The owning Center/program.
- c. The physical location to include defining the whole or partial facility.
- d. The responsible enterprise.
- e. Whether the asset is part of the Agency continuity of operations planning program.
- f. Contingency plans to ensure sufficient redundancies exist for key systems and infrastructure elements. Plans should be reviewed/vetted through all key stakeholder organizations.

3.2.4 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. 3.2.5 Project and program managers are responsible for reporting incidents or perceived incidents involving loss of sensitive mission information to the Center Protective Services Office.

3.3 OPSEC

3.3.1 NSDD 298: National Operations Security Program establishes the National OPSEC Program and requires executive departments or agencies supporting national security classified or sensitive missions to establish a formal OPSEC program. 3.3.2 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.

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

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

3.4 Risk Management Process

3.4.1 The AA, OPS in coordination with the concerned directories, programs, projects, and Centers shall establish and implement an Enterprise Security Risk Management Program that enhances operational readiness and mission success by providing security support to program/projects throughout the life cycle of a system or activity that is commensurate with the risk and helps ensure mission critical information, technologies, and/or assets are appropriately protected.

3.4.2 NASA has adopted a risk management approach, using requirements established in NPR 8000.4A, Agency Risk Management Procedural Requirements, NPR 1620.2, Facility Security Assessments, and NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, in which the risk must be weighed against the cost and operational impact of implementing established minimum-security standards.

3.4.3 Risk management provides a mechanism that allows security and program/project managers to recommend waivers to security standards based upon a threat and vulnerability assessment and the resulting risk determination.

3.4.4 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.

3.4.5 The CCPS/CCS shall ensure that security and program standards, established in this and other NPRs are met or that appropriate requests for exception or waivers are submitted and approved by the AA, MSD.

3.5 Special Security Programs

3.5.1 All NASA security activity associated with Special Security Programs are authorized and prescribed by the NASA Special Access Program Security Guide (SAPSG). Furthermore, NPD 1600.4, National Security Programs, establishes policy for Special Access Programs (SAP).

3.5.2 Sensitive Compartmented Information (SCI) Programs.

3.5.2.1 SCI programs shall only be created within NASA upon specific written approval of the AA, OPS or his designated representative to ensure required security protocols are implemented and maintained. Furthermore, NPD 1600.4, National Security Programs, establishes policy for SCI programs.

3.5.2.2 All requests for NASA personnel, including NASA contractors, to participate in SCI programs external to NASA must be coordinated with the AA, OPS or his/her designated representative to ensure accountability of NASA equities.

3.5.2.3 Failure to comply with the requirements of this section shall result in denial or revocation of security clearance and suspension of SCI activity.

3.6 NASA Critical Infrastructure (NCI) and Key Resources Identification, Prioritization, and Protection

3.6.1 PPD-21 "Critical Infrastructure Security and Resilience" 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 NCI to better facilitate designation of vital "mission oriented" critical infrastructure and key resources.

3.6.2 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.

3.6.3 Designated NCI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate physical security risk vulnerability assessment. At a minimum, NCI will be designated Facility Security Level III as defined in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

3.6.4 NCI may include IT resources; critical components, communication, command, and control capability, Government-owned flight or experimental flight vehicles, International Space Station and apparatus, and one-of-a-kind irreplaceable facilities.

3.6.5 Supporting infrastructure called "interdependencies" shall not be designated as NCI.

3.6.5.1 "Interdependencies" includes those external and internal commercial elements that the Center NCI depends on to operate, including electrical power, gas, communications hubs, local area networks, and telephone systems.

3.6.5.2 "Interdependencies" nevertheless shall 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" will also take the "single point of failure" aspect into account when developing their mitigation plans.

3.6.6 Policy and procedures shall be developed and implemented at each Center that accurately reflect Agency requirements for assessing NCI as outlined in this and other Agency-wide requirements. This ensures Agency-wide uniformity and consistency in the approach to performing the appropriate security risk assessments for each identified NCI.

3.6.7 Criteria and procedures NASA Centers shall use in identifying NCI are contained in Appendix F, Identifying and Nominating NASA Assets for the NASA Critical Infrastructure Protection Program (NCIPP).

3.6.8 Minimum security requirements for NCI facilities or facilities housing NCI assets are provided in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

[TOC](#)	[Preface](#)	[Chapter1](#)	[Chapter2](#)	[Chapter3](#)	[Chapter4](#)	[Chapter5](#)	[Chapter6](#)
[AppendixA](#)	[AppendixB](#)	[AppendixC](#)	[AppendixD](#)	[AppendixE](#)	[AppendixF](#)		
[AppendixG](#)	[AppendixH](#)	[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>
