



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A

Effective Date: May 16, 2006

Expiration Date: November
16, 2016

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

Request Notification of Change (NASA Only)

Subject: Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)

Responsible Office: Office of the Chief Information Officer

[| TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

Chapter 1 - Information Security Management

1.1 Overview

1.1.1 This NPR establishes the information security requirements and responsibilities for NASA, relative to the policy set forth in NPD 2810.1, NASA Information Security Policy. This NPR does not negate any existing policies, procedures, memos, handbooks, etc. except where explicitly stated in section P.6 Cancellation. This document is intended to provide a framework for information security and serve as an avenue for the authorization of more in-depth documents (e.g., handbooks, memos).

1.1.2 This NPR is organized into four major sections: (1) Preface; (2) Overview; (3) security control chapters; and (4) Appendices.

1.1.2.1 The security control chapters satisfy requirements related to policy as described by NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations. Every control family is addressed in its own chapter.

1.1.2.2 Each security control chapter defines the overall intent of the control family, roles and responsibilities specific to the control family, and provides references to where more detailed requirements, procedures, and information may be found.

1.1.3 FISMA defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

1.1.4 The Clinger-Cohen Act states that the NIST Federal Information Processing Standards (FIPS) are "compulsory and binding" 40 U.S.C. § 11331(b) (1) (C). FISMA also advocates that security be based on "periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency." 44 U.S.C. § 3544(b) (1). Furthermore, FISMA provides flexibility regarding the application of security controls.

1.1.5 To implement federal and NASA policies and requirements, FISMA allows for the delegation of responsibilities into various functional roles.

1.1.6 NASA senior management establishes the Agency's information security program and its overall objectives and priorities. NASA Headquarters, Centers, satellite facilities, and support service contractor sites have the latitude to use their internal organizational structure to fulfill the roles and responsibilities described herein if the approach is documented in a formal policy.

1.1.7 This NPR accomplishes the aforementioned requirements of FISMA as it relates to NASA information and information systems.

1.1.7.1 This NPR supports NASA's implementation of a risk management framework (RMF).

1.1.7.2 A solid understanding of the RMF core tenets is critical to NASA's ability to securely identify, understand, and manage risk.

1.1.7.3 The RMF focuses on the concepts of near real-time risk management, continuous monitoring of information security postures, the automation and enterprise consolidation of common security objectives, and the selection, implementation, assessment, and monitoring of security controls.

1.1.7.4 The most critical underlying feature of the RMF is the concept that security practices are governed by the balanced understanding of information security postures and the impact of their potential compromise on the Agency's mission needs and objectives.

1.2 Roles and Responsibilities

1.2.1 The following are overarching roles and responsibilities related to NASA's information security program. Specific roles and responsibilities, as related to security controls, are referenced throughout the remainder of this NPR in their respective chapters.

1.2.2 Throughout this document roles and responsibilities are generally listed at the highest level possible, with the operating assumption that specific tasks and functions may be delegated as necessary unless explicitly prohibited.

1.2.3 The requirement that certain roles be filled by employees of the United States Federal Government is generally waived for JPL, which is largely operated and managed by contracted personnel.

1.2.3.1 The NASA Administrator shall ensure the security of NASA's information and information systems.

1.2.3.2 The NASA Chief Information Officer (CIO) shall:

- a. Ensure compliance with applicable federal and NASA information security program requirements.
- b. Develop and maintain a NASA-wide information security program.
- c. Designate a Senior Agency Information Security Officer (SAISO).
- d. Commission an Information Technology Security Advisory Board (ITSAB).
- e. Evaluate and approve the designation of Authorizing Officials (AO).
- f. Advise senior NASA officials concerning their information security responsibilities.
- g. Ensure the NASA enterprise architecture integrates information security considerations into the strategic, capital, and investment planning process.
- h. Encourage the maximum reuse and sharing of security-related information throughout the NASA community.
- i. Issue NASA Information Technology Requirements (NITRs) documents to keep the NASA information security program current with changes in the information security environment and with changes in federal policy and guidelines, as needed.
- j. Ensure that NITRs are incorporated into future versions of the NPR and that once a NITR has been incorporated into the next revision, the NITR is to be canceled.
- k. Be an employee of the United States Federal Government.

1.2.3.3 The Center/Executive Director shall appoint the Center Chief Information Security Officers (CISOs) to assist the Center CIO by providing organization and direction for implementing the NASA information security program.

1.2.3.4 The Center CIO shall:

- a. Execute the responsibilities of the NASA CIO as applicable at the Center level.
- b. Assign Organizational Computer Security Official (OCSO) to facilitate the implementation and oversight of information security within their organization.
- c. Be an employee of the United States Federal Government.

1.2.3.5 The Senior Agency Information Security Officer (SAISO) shall:

- a. Carry out the responsibilities of the NASA CIO under FISMA, and federal and NASA information security program requirements.
- b. Establish and maintain an office with the mission and resources to ensure compliance with federal and NASA information security program requirements.
- c. Serve as the NASA CIO's primary liaison with Center CISO, AOs, Information System Owners (ISO), and

Information System Security Officers (ISSO).

- d. Manage the NASA information security program.
- e. Oversee and arbitrate conflict resolution, relative to information security concerns, for all NASA-wide information systems .
- f. Ensure the planning of a framework for the use and adoption of current and new information security technologies implemented throughout the Agency.
- g. Interact with internal and external resources to coordinate information security compliance across the Agency.
- h. Ensure that NASA develops, disseminates, reviews annually, and appropriately updates policy, procedure, and technical documentation as related to information security.
- i. Establish and maintain a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA's information security program.
- j. Maintain and update, as needed to comply with federal and NASA requirements, NPD 2810.1, NASA Information Security Policy; NPR 2810.1, Security of Information Technology; and all related handbooks.
- k. Authorize NASA information technology security handbooks (ITS-HBK).
- l. Publish and maintain information security handbooks which will provide detailed information and guidance regarding the processes to meet the requirements of this NPR.
- m. Be an employee of the United States Federal Government.

1.2.3.6 The Center Chief Information Security Officer (CISO) shall:

- a. Execute the responsibilities of the SAISO as applicable at the Center level.
- b. Ensure compliance with information security requirements relative to all personnel, information and information systems that are resident at their Center, managed from their Center, or associate with a contract, grant, purchase order, or cooperative agreement managed at their Center.
- c. Oversee information security operations, governance, architecture, and engineering to ensure Center compliance with federal and NASA information security requirements.
- d. Ensure that feedback from ISOs, ISSOs, and other information security personnel as to the impact of the policies, procedures, and framework is actively solicited and provided to the SAISO for consideration.
- f. Be an employee of the United States Federal Government.

1.2.3.7 The Organizational Computer Security Official (OCSO) shall:

- a. Ensure organization-level compliance with information security requirements.
- b. Serve as their organization's representative to the Center CISO on information security matters.
- c. Report the status of the organization's information security to the Center CISO and senior organization officials.
- d. Ensure compliance with NASA and Center information security requirements.
- e. Be an employee of the United States Federal Government.

1.2.3.8 The Authorizing Official (AO) shall:

- a. Formally assume the responsibility for the operation of an information system.
- b. Allocate sufficient resources to adequately protect information and information systems based on an assessment of organizational risks.
- c. Oversee the budget and business operations of organizational information systems.
- d. Assign Authorizing Official Designated Representatives (AODR) as necessary. Note: The responsibility of signing formal Authorizations to Operate (ATO) may not be delegated.
- e. Be an employee of the United States Federal Government.

1.2.3.9 The Authorizing Official Designated Representative (AODR) shall:

- a. Execute the responsibilities of the AO as delegated.
- b. Be an employee of the United States Federal Government.

1.2.3.10 The Information System Owner (ISO) shall:

- a. Acquire, develop, integrate, operate, modify, maintain, and dispose of information systems.
- b. Ensure system-level implementation of all Agency and Center requirements.
- c. Ensure that security controls are implemented according to a thorough risk-based analysis of their information systems' security postures.
- d. Provide necessary assessment documentation, as required. .
- e. Ensure information systems are categorized in a manner that reflects the criticality of their function, and the sensitivity of the information they generate, collect, process, store, or disseminate.
- f. Take appropriate actions to identify, and minimize or eliminate information system security deficiencies and weaknesses.
- g. Allocate resources to protect information and information systems based on an assessment of system risks.
- h. Communicate feedback to the Center CISO, and AO regarding the impact of Agency and Center-wide information security requirements on the operation of their information systems.
- i. Ensure funding requests for information security requirements are included in annual budgeting submissions.
- j. Utilize, to the extent possible, Agency provided infrastructure.

1.2.3.11 The Information Owner/Steward (IO) shall:

- a. Exercise statutory or operational authority for specified information.
- b. Ensure the selection of security controls for the generation, collection, processing, dissemination, and disposal of information under their authority.
- c. Fulfill the responsibilities of the ISO for NASA external information systems, as necessary.

1.2.3.12 The Information System Security Officer (ISSO) shall:

- a. Serve as the principal advisor to the ISO on issues regarding information security.
- b. Ensure an appropriate operational security posture is maintained for their information system.
- c. Be responsible for the day-to-day security operations of their information system.

1.2.3.13 The NASA User shall comply with all policy and procedures as required by this NPR.

| [TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [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>
