| NODIS Library | Legal Policies(2000s) | Search |

NASA
Procedural
Requirements

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: July 16, 2021

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

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

Responsible Office: Office of the Chief Information Officer

Table of Contents

Change History

Preface

Chapter 1 Information Security Management

Chapter 2 Management Controls

Chapter 3 Operational Controls

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Change History

NPR 2810.1A, Security of Information Technology

Chg#	Code/Center	Approved	Description/Comments
1	**JA**	05/19/2011	Removed Chapter 1 Introduction, Laws and Regulations, Capital Planning and Metrics, and moved Roles & Responsibilities to Chapter 2. Review and updated document for NPR 1400 compliance. Clarify roles and responsibilities CIO office.
2	JA	04/23/2012	Administrative corrections made to ITS HBK citations listed in P.4 Applicable Documents.

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.

Preface

P.1 Purpose

The purpose of this document is to:

a. Establish the information security requirements for the National Aeronautics and Space Administration (NASA) relative to the policy set forth in NASA Policy Directive (NPD) 2810.1, NASA Information Security Program. The procedural requirements, herein prescribe roles, responsibilities, and conditions that directly or indirectly promote information security throughout the life cycle of all NASA information and information systems.

b. Identify information security policies, procedures, and practices which are appropriate to NASA's mission, and are consistent with applicable federal laws, executive orders, directives, policies, and regulations.

c. Serve as a reference to the NASA community regarding specific information security roles and responsibilities, and provide resources where more detailed information may be found.

d. Satisfy security policy guidance as outlined by National Institute of Standards Technology (NIST), Special Publication (SP) 800-53. Recommended Security Controls for Federal Information Systems and Organizations.

P.2 Applicability

a. This NASA Procedural Requirement (NPR) applies to:

(1) NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers.

(2) For purposes of this NPR, NASA Headquarters is treated as a Center. Further, all roles and responsibilities of a Center Chief Information Officer (CIO) are also applicable to the NASA Headquarters CIO and all stipulated Center requirements are also applicable to NASA Headquarters.

(3) NASA Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

(4) This NPR applies to unclassified NASA information and information systems, including those that are contracted out or outsourced to (1) a Government owned, contractor operated (GOCO) facility; (2) partners under the Space Act; (3) partners under the Commerical Space Act of 1997; or (4) commercial or university facilities.

(5) Information systems that do not process NASA information, or are merely incidental to a contract (e.g., a contractor's payroll and personnel management system) are normally excluded from full review or audits, to protect proprietary and private data.

(6) This NPR does not apply to Classfied National Security Information (CNSI). CNSI is the responsibility of the Office of Protective Services and is covered under CNSI policy and

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

requirements contained in NPD 1600.2, NASA Security Policy and NPR 1600.1, NASA Security Program Procedural Requirements.

P.3 Authority

a. 5 U.S.C. § 552, et seq., the Freedom of Information Act, as implemented by 14 C.F.R.§ 1206, Availability of Agency Records to Members of the Public, as amended.

b. 5 U.S.C. § 552a, the Privacy Act, Pub. L. No. 93-579.

c. 5 U.S.C. App. III, Inspector General Act of 1978.

d. 18 U.S.C. § 799, Violation of Regulations of National Aeronautics and Space Administration, as amended.

e. 18 U.S.C. § 2510, et seq., Electronic Communications Privacy Act of 1986, as amended.

f. 22 U.S.C. § 2751, et seq., Arms Export Control Act, as implemented by 22 C.F.R. § 120-130, International Traffic in Arms Regulations.

g. 40 U.S.C. § 11101 et seq., Chapter 808 of Pub. L 104-208, the Clinger-Cohen Act of 1996.

h. 42 U.S.C. § 201 nt., Health Insurance Portability and Accountability Act of 1996, as amended.

i. 44 U.S.C. § 101, E-Government Act of 2002.

j. 44 U.S.C. § 3535, Federal Information Security Management Act (FISMA) of 2002.

k. 44 U.S.C. § 3501, et seq., Paperwork Reduction Act of 1995, as amended.

l. 50 U.S.C. Appendix 2401-2420, Export Administration Act of 1979, as amended.

m. 51 U.S.C. § 20113(e), The National Aeronautics and Space Act of 1958, as amended.

n. EO 12958, Classified National Security Information, dated April 17, 1992.

o. EO 13011, Federal Information Technology, dated July 16, 1996.

p. 14 C.F.R § 1206, Availability of Agency Records to Members of the Public.

q. 15 C.F.R § 730-774, Export Administration Regulations.

r. 22 C.F.R § 120-130, International Traffic in Arms Regulations.

P.4 Applicable Documents

a. FIPS 140, Security Requirements for Cryptographic Modules.

b. FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

c. HSPD-12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 2004.

d. HSPD-20, National Continuity Policy.

e. NIST SP 800-30, Risk Management Guide for Information Technology Systems.

f. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

g. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

h. NIST SP 800-46, Guide to Enterprise Telework and Remote Access Security.

i. NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

j. NIST SP 800-61, Computer Security Incident Handling Guide.

k. NIST SP 800-63, Electronic Authentication Guideline.

l. NIST SP 800-83, Guide to Malware Incident Prevention and Handling.

m. NIST SP 800-88, Guidelines for Media Sanitization.

n. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

o. X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.

p. NPD 1600.2, NASA Security Policy.

q. NPD 1600.3, Policy on Prevention of and Response to Workplace Violence.

r. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

s. NPD 2810.1, NASA Information Security Policy.

t. NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedural Requirements.

u. NPR 1382.1, NASA Privacy Procedural Requirements.

v. NPR 1441.1, NASA Records and Retention Schedule.

w. NPR 1600.1, NASA Security Program Procedural Requirements.

x. NPR 1620.2, Physical Security Vulnerability Risk Assessments.

y. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

z. NPR 2800.1, Managing Information Technology.

aa. NPR 2841.1, Identity, Credential, and Access Management Services.

bb. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

cc. NPR 8000.4, Agency Risk Management Procedural Requirements.

dd. NPR 8820, Facility Project Requirements.

ee. NPR 8831.2, Facilities Maintenance and Operations Management.

ff. ITS-HBK-2841.001, Identity, Credential, and Access Management (ICAM) Services Handbook.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

gg. ITS-HBK-2810.02, Security Assessment and Authorization.

hh. ITS-HBK-2810.03, Planning.

ii. ITS-HBK-2810.04, Risk Assessment.

jj. ITS-HBK-2810.05, System and Services Acquisition.

kk. ITS-HBK-2810.06, Security Awareness and Training.

ll. ITS-HBK-2810.07, Configuration Management.

mm. ITS-HBK-2810.08, Contingency Planning.

nn. ITS-HBK-2810.09, Incident Response and Management.

oo. ITS-HBK-2810.10, Maintenance.

pp. ITS-HBK-2810.11, Media Protection.

qq. ITS-HBK-2810.12, Physical and Environmental Protection.

rr. ITS-HBK-2810.13, Personnel Security.

ss. ITS-HBK-2810.14, System and Information Integrity.

tt. ITS-HBK-2810.15, Access Control.

uu. ITS-HBK-2810.16, Audit and Accountability.

vv. ITS-HBK-2810.17, Identification and Authentication.

ww. ITS-HBK-2810.18, System and Communication.

P.5 Measurement/Verification

a. The obligation to measure performance and reduce cost is driven by Federal regulatory and NASA requirements. These measurements shall be based upon NASA's goals and objectives, be designed to provide substantive justification for decision-making, and be utilized to measure the effectiveness of the information security program, policies, and requirements. Information security program measurement goals and objectives are not static and will be adjusted as the operating environment, threats, and requirements evolve.

b. The Office of the CIO shall provide assessments/audits of the application of this NPR. This will consist of periodic reporting from the Centers, including information collected for the satisfaction of Office of Management and Budget (OMB) and the Federal Information Security Management Act (FISMA) reporting requirements.

c. All covered entities are subject to information security compliance reviews and audits by NASA.

P.6 Cancellation

a. NPR 2810.1, Security of Information Technology, August 12, 2004

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

b. NITR-2810-12, Continuous Monitoring, May 18, 2008

c. NITR-2810-14, Managing Elevated User Privileges on NASA IT Devices, August 17, 2009

d. NITR-2810-15, Contingency Planning, June 9, 2008

e. NITR-2810-17, System Maintenance Policy and Procedures, November 12, 2008

f. NITR-2810-19, Audit and Accountability Policy and Procedures, November 12, 2008

g. NITR-2810-20, System and Communications Protection Policy and Procedures, March 11, 2009

h. NITR-2810-21, System and Services Acquisition Policy and Procedures, April 28, 2009

i. NITR-2810-22, Media Protection Policy and Procedures, January 7, 2009

j. NITR-2810-23, NASA Authorizing Official (AO) Procedural Requirements, March 1, 2009

k. NITR-2810-24, NASA IT Device Vulnerability Management, January 28, 2010

Revalidated May 19, 2011, Original signed by:

/S/
Patricia Dunnington
Chief Information Officer

DISTRIBUTION: NODIS

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

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

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

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

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

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

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.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Chapter 2 - Management Controls

2.1 Program Management (PM)

2.1.1 The Program Management control family relates to the legal requirements that NASA develop, document, and implement a comprehensive program under the direction of senior management, to provide security for information and information systems. The information security program is required to include ongoing assessments of the risk and magnitude of the harm that could result from compromise to Agency information systems' confidentiality, integrity, and availability. Such risk assessments, when addressed throughout the information system life cycle, can cost-effectively help to reduce information security risks.

2.1.2 The tenets and framework of NASA's information security program are spelled out in this NPR and its referenced security handbooks. The policies, procedures, milestones, metrics, and responsibilities of the information security program together make up the information security program plan.

2.1.3 Program Management Policy

2.1.3.1 The NASA CIO shall:

a. Report periodically to the NASA Administrator on the effectiveness of NASA's information security program, including the progress of remedial actions.

b. Ensure the development and maintenance of a NASA-wide information system inventory.

c. Report to OMB on the status of NASA's information security program, as required.

2.1.3.2 The SAISO shall:

a. Develop and document a NASA-wide information security program which includes an overview and descriptions of measures of performance, enterprise security architecture, critical infrastructure, risk management strategy, and an information security assessment and authorization process.

b. Continuously review, update, and augment the information security program as necessary.

c. Ensure that the information security program plan, policy, and requirements are implemented.

d. Define a process for the development, documentation, and maintenance of plans of action and milestones (POA&M) and for the acceptance of risk.

e. Establish and manage a NASA-wide information security performance metrics program.

f. Coordinate information security reviews with the NASA Office of the Inspector General (OIG) and other external entities such as the U.S. Government Accountability Office (GAO).

2.2 Security Assessment and Authorization (CA)

2.2.1 The Security Assessment and Authorization control family relates to the activities and requirements surrounding the routine testing of security controls, the continuous monitoring of system security posture, and the ongoing risk-based decisions to approve or deny the use of a system. Officials within the NASA community are responsible for continuously ensuring the effectiveness of security control implementations throughout the life cycle of a system. Moreover, in light of an ever-changing security landscape, designated NASA officials should always be prepared to determine the impact of a system's operation on the success of the NASA mission.

2.2.2 Security Assessment and Authorization procedures shall be governed by ITS-HBK-2810.02, Security Assessment and Authorization.

2.2.3 Security Assessment and Authorization Policy

2.2.3.1 The NASA CIO shall ensure information security control assessments, security authorizations, and OMB and FISMA reporting directives are completed across the Agency in a timely and cost-effective manner.

2.2.3.2 The SAISO shall:

a. Ensure the assessment, updating, and dissemination of information regarding Agency Common Controls.

b. Ensure the assessment, updating, and dissemination of information regarding those portions of Hybrid Controls which the Agency implements.

c. Ensure the annual updating and dissemination of Organizationally-Defined Values via an OCIO memorandum or handbook update.

d. Provision a NASA-wide repository for information security documentation.

e. Ensure the identification and management of common threats to NASA.

f. Ensure compliance with OMB and FISMA reporting requirements.

2.2.3.3 The Center CISO shall:

a. Verify the proper application of information system categorization criteria and requirements.

b. Ensure the identification and management of common threats to their Center.

2.2.3.4 The OCSO shall:

a. Verify the proper application of information system categorization criteria and requirements for their organization.

b. Ensure the identification and management of common threats to their organization.

2.2.3.5 The AO shall:

a. Ensure that all systems undergo a complete system security assessment prior to granting an initial ATO.

b. Approve or reject information system categorizations.

c. Grant or deny systems ATO based on an evaluation of risk to the security posture of their information systems.

d. Make decisions with regard to the planning and resourcing of information security assessment and authorization activities.

2.2.3.6 The ISO shall:

a. Ensure capabilities to continuously monitor the security posture of their information system.

b. Ensure the creation of POA&Ms, or provide a documented acceptance of risk related to any identified system security deficiencies or weaknesses.

c. Ensure the maintenance of security documentation in the NASA-wide security document repository.

d. Maintain and update formal documentation regarding system interconnections.

e. Ensure the availability of resources for assessment and authorization activities.

f. Ensure the completion of POA&M items.

g. Inform key officials of pending assessment and authorization activities.

h. Seek an ATO from the AO prior to the operation of a new system, and maintain an ongoing authorization thereafter, in accordance with a risk-based approach to security.

2.2.3.7 The IO shall categorize information and ensure, in collaboration with the ISO, that information system categorizations appropriately reflect the information they generate, collect, process, and disseminate.

2.3 Planning (PL)

2.3.1 The Planning control family relates to the definition and documentation of the key resources and activities used to protect Agency information system resources. Effective security planning is both comprehensive and flexible. NASA uses a System Security Plan (SSP) template that specifies the set of information controls that must be considered for each system. The plan content for any specific system is governed by a risk assessment of the particular threats facing the system and a tailoring of security controls to meet those threats.

2.3.2 NASA follows the requirements of FIP 199, Standards for Security Categorization of Federal Information and Information Systems.

2.3.3 Security Planning procedures shall be governed by NPR 1382.1, NASA Privacy Procedural Requirements; ITS-HBK-2810.03, Planning.

2.3.4 Planning Policy

2.3.4.1 The SAISO shall identify a NASA-wide resource for the management of corrective action plans to mitigate information system security weaknesses.

2.3.4.2 The OCSO shall ensure that their organization's SSPs are reviewed and updated in accordance with this NPR and its associated handbooks.

2.3.4.3 The AO shall approve SSPs under their authority.

2.3.4.4 The ISO shall:

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

a. Ensure that all SSPs are developed and tailored to address the threats and associated risks faced by the system.

b. Develop Memoranda of Agreements (MOA), Memoranda of Understandings (MOU), and Interconnection Security Agreements (ISA) for their systems as applicable.

c. Develop and maintain a SSP for their information systems.

d. Ensure that SSPs are reviewed and updated in accordance with this NPR and its associated handbooks.

e. Establish rules of behavior for their systems as required.

2.4 Risk Assessment (RA)

2.4.1 The Risk Assessment control family relates to a framework for the identification, tracking and mitigation of information security risks. The goal of effective risk management is to articulate the risk that threats may have on Agency owned assets, data and personnel, and to minimize the risk by applying security controls.

2.4.2 In order to make informed decisions about the security of Agency assets and personnel, all Agency security roles share the responsibility of understanding the risks that affect their information and information systems, and the mitigating controls which address them. All roles are responsible for communicating risks to the level necessary to satisfy all potential stakeholders.

2.4.3 NASA utilizes the guidelines of NIST SP 800-30, Risk Management Guide for Information Technology Systems; and NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems.

2.4.4 Risk Assessment procedures shall be governed by NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; NPR 8000.4, Agency Risk Management Procedural Requirements; and ITS-HBK-2810.04, Risk Assessment.

2.4.5 Risk Assessment Policy

2.4.5.1 The SAISO shall define and make available a RMF that describes a uniform methodology for risk assessment that is applicable to all Agency internal and external systems.

2.4.5.2 The Center CISO shall understand and communicate, with the AO and ISO, any risks associated with any information system which may pose an unacceptable level of risk to Agency operations and resources.

2.4.5.3 The AO shall ensure that only systems posing an acceptable level of risk to Agency assets, data, and personnel are approved for production operation.

2.4.5.4 The ISO shall:

a. Ensure that their information systems are assessed for risk in accordance with Agency policy and procedures.

b. Ensure resources are applied towards the mitigation of identified risks to minimize risk.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

c. Ensure that systems that are identified as posing unacceptable risk to other Agency operations or resources are communicated to the Center CISO and AO and mitigated in a manner that ensures the protection of Agency assets, data, and personnel.

2.5 System and Services Acquisition (SA)

2.5.1 The System and Services Acquisition control family relates to the need to adequately plan for, appropriately fund, and efficiently acquire the resources necessary to maintain information security. The control family defines the actions that best enable NASA's security program to make effective use of externally-sourced expertise and tools. Furthermore, it mandates that security considerations not be treated as an afterthought, but are instead addressed early-on in parallel with funding and design decisions.

2.5.2 System and Services Acquisition procedures shall be governed by ITS-HBK-2810.05, System and Services Acquisition.

2.5.3 System and Services Acquisition Policy

2.5.3.1 The SAISO shall:

a. Include information security resource requirements in programming and budgeting documentation.

b. Work with the NASA Office of Procurement to oversee the development and maintenance of an information security clause and coordinate its implementation in the NASA Federal Acquisition Regulations (FAR) with the NASA Office of Procurement.

2.5.3.2 The ISO shall:

a. Ensure that required System and Services Acquisition policy and procedures are implemented for their information systems and documented in the associated SSPs.

b. Ensure information security considerations are managed throughout their systems' development life cycle.

c. Ensure that the appropriate information security requirements are articulated in solicitations and resulting contracts for acquisitions made in support of their systems. Note: The principal information security clause to be included with contracts, grants, and other agreements is defined by the FAR clause and applicable Procurement Information Circular IT Security Requirements.

2.5.3.3 The IO shall assist in the development of security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information.

2.5.3.4 The ISSO shall assist in the development of security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information systems.

2.5.3.5 The Assistant Administrator of Procurement shall:

a. Ensure that contracting officials are aware of requirements related to information security.

b. Ensure the inclusion of information security requirements in all contracts and solicitations.

Chapter 3 - Operational Controls

3.1 Awareness and Training (AT)

3.1.1 The Security Awareness and Training control family relates to the information security knowledge requirements for all users of Agency information and information systems, and the development and delivery of courses and other training resources to enable and validate satisfaction of those requirements. Satisfaction of training requirements is a precursor to access controls for NASA information system resources.

3.1.2 Security Awareness and Training procedures shall be governed by ITS-HBK-2810.06, Security Awareness and Training.

3.1.3 Security Awareness and Training Policy

3.1.3.1 The NASA CIO shall:

a. Develop, maintain, and promote NASA-wide information security awareness and training.

b. Complete any role-based training activities required of their position.

3.1.3.2 The SAISO shall:

a. Define and make available all Agency security awareness and training requirements. This includes general knowledge requirements that pertain to all NASA users as well as role-based requirements targeted at managers, information security professionals, etc.

b. Define educational courses and materials that can be used to satisfy Agency security awareness and training requirements.

c. Oversee the fulfillment of training requirements across the Agency.

d. Complete any role-based training activities required of their position.

3.1.3.3 The Center CISO shall:

a. Track and report on the completion of security awareness and training requirements at the Center level.

b. Complete any role-based training activities required of their position.

3.1.3.4 The OCSO shall:

a. Track and report on the completion of security awareness and training requirements at the organizational level.

b. Complete any role-based training activities required of their position.

3.1.3.5 The ISO shall:

a. Ensure only users who comply with all Agency information security awareness and training requirements are allowed access to the ISO's information system(s).

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

b. Ensure all personnel supporting the information system whose roles include significant information security responsibilities comply with the applicable role-based security awareness and training requirements.

c. Complete any role-based training activities required of their position.

3.1.3.6 The NASA User shall:

a. Be responsible for maintaining compliance with applicable security and awareness training requirements, in accordance with role-based security awareness and training requirements.

b. Ensure their training results are recorded in the designated NASA-wide training platform.

3.1.3.7 The Assistant Administrator of the Office of Human Capital Management shall ensure the availability of a NASA-wide platform for training delivery, as well as training results and records management.

3.2 Configuration Management (CM)

3.2.1 The Configuration Management control family relates to the organizational aspects of information system baseline configurations, establishing review and validation, and change control. The control family also manages administrator roles, and the ability of individuals to make changes to the information systems' configuration.

3.2.2 The concept of configuration management is critical to the continuous monitoring processes. Strict methodologies for the regulation of information system baselines and changes to system configurations are necessary for near real-time understanding of a system's risk posture.

3.2.3 Configuration Management procedures shall be governed by NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; and ITS-HBK-2810.07, Configuration Management .

3.2.4 Configuration Management Policy

3.2.4.1 The SAISO shall:

a. Ensure that processes for development, approval, distribution, and verification of security configuration baselines, which are common to all information system components within the Agency, exist and are effective.

b. Ensure that processes are in place to monitor security baseline configuration compliance.

c. Ensure security baseline configurations conform to applicable federal requirements (e.g., Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB)).

3.2.4.2 The ISO shall:

a. Maintain an information system inventory.

b. Ensure all information system components are incorporated into and maintained in the NASA-wide information system inventory.

c. Create, implement, and maintain configuration change control policies and processes for their

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

system as needed.

d. Perform an information system risk analysis to support development of Agency security configuration baselines.

3.2.4.3 The ISSO shall perform an information system risk analysis to justify system configurations and support the process of continuous monitoring.

3.3 Contingency Planning (CP)

3.3.1 The Contingency Planning control family relates to the preparation of information security response, recovery, and continuity activities to avoid disruptions to critical business processes. Successful contingency planning increases the likelihood that essential information and information systems will be available and assists an organization with maintaining continuity of operations in emergency situations. Effective contingency planning, training, testing, and execution are essential to mitigating the impacts resulting from system and service disruptions.

3.3.2 NASA follows the requirements of HSPD-20, National Continuity Policy .

3.3 .3 NASA utilizes the guidelines of NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

3.3 .4 Contingency Planning procedures shall be governed by NPR 1040.1, NASA Continuity of Operations Planning (COOP) Procedures and Guidelines ; and ITS-HBK-2810.08, Contingency Planning.

3.3.5 Contingency Planning Policy

3.3.5.1 The Center CIO shall c oordinate Center-wide contingency planning efforts which provide for notification, activation, response, recovery, and reconstitution of a Center's information systems as a result of damage or disruption caused by a man-made or natural disaster.

3.3.5.2 The SAISO shall:

a. Develop and maintain Agency-level information system contingency planning policies, procedures, and guidance for NASA.

b. Ensure that NASA has appropriate and tested information security contingency plans in place to continue fulfilling the business functions of NASA in support of the Agency's mission essential functions.

c. Ensure that Center CISOs are coordinating a Center-based information system contingency program.

d. Establish recovery metrics and objectives for information systems.

e. Ensure fulfillment of OMB and FISMA contingency plan testing requirements.

3.3.5.3 The Center CISO shall:

a. Ensure implementation of those information system contingency planning policies and procedures which provide for notification, activation, response, recovery, and reconstitution.

b. Oversee and arbitrate conflict resolution for all Center-wide information system contingency

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

plans .

c. Ensure and support information system contingency plan tests, training, and exercises.

3.3.5.4 The ISO shall:

a. Be responsible for developing, testing, implementing, and maintaining information system contingency plans.

b. Ensure that assessment, recovery, and restoration procedures are formally documented.

c. Be responsible for ensuring that the contingency plan documentation is maintained in a ready state and accurately reflects system requirements, procedures, organizational structure, and policies.

d. Ensure that recovery and restoration procedures outlined in information system contingency plans satisfy a risk-based analysis of the business needs and objectives of the information system and Agency at large.

e. Ensure that information system contingency plan documentation is at a level appropriate to permit a coordinated response at the Center and/or the Agency level as applicable.

f. Be responsible for ensuring that contingency plans are tested, evaluated, and documented appropriately for accuracy, completeness, and effectiveness via a periodic test, training, and exercise program.

3.4 Incident Response and Management (IR)

3.4.1 The Incident Response and Management control family relates to dealing with the potential for and actual damage and disruption to information systems. An "incident" is any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information.

3.4.2 Preventative activities based on the results of risk assessments can lower the number of incidents; however, they will not prevent all incidents. Therefore, an incident response and management capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. The NASA Security Operations Center (SOC) provides centralized Agency coordination for information security incident management, response preparation, identification, analysis, communication, containment, eradication, recovery, and follow-up activities.

3.4.3 NASA utilizes the guidelines of NIST SP 800-61, Computer Security Incident Handling Guide; and NIST SP 800-83, Guide to Malware Incident Prevention and Handling.

3.4.4 Incident Response and Management procedures shall be governed by ITS-HBK-2810.09, Incident Response and Management.

3.4.5 Incident Response and Management Policy

3.4.5.1 The NASA CIO shall allocate resources for a NASA-wide SOC.

3.4.5.2 The Center CIO shall:

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

a. Establish an incident response team for their Center.

b. Ensure capability to support information security investigations.

3.4.5.3 The SAISO shall:

a. Develop and maintain a NASA-wide process for detecting, reporting, and responding to information security incidents.

b. Ensure support of investigations into information security incidents conducted by OIG, and the Office of Protective Services (OPS) related to criminal activity, counterintelligence, or counterterrorism.

c. Ensure support of investigations into information security incidents initiated by the Office of the General Counsel, the office of Human Capital Management, a Center's Office of Human Resources, and a Center's Office of the Chief Counsel.

d. Refer any suspected criminal, counterintelligence, or counterterrorism activity to the OIG and OPS, respectively, as appropriate.

e. Implement and manage a NASA-wide SOC.

f. Oversee all activities related to incident response and management.

g. Ensure that incidents are appropriately reported to external agencies as directed by applicable laws and regulations.

3.4.5.4 The Center CISO shall:

a. Provide oversight of the incident response and management policies, procedures, investigations, and reporting for all information systems at their Center.

b. Provide oversight of the incident response tests, training, and exercises for their Center information systems.

c. Ensure coordination between the incident response team and the Center privacy managers regarding breach response, and handling of incidents related to sensitive information.

3.4.5.5 The ISO shall:

a. Designate individuals responsible for incident response reporting and management of their information system.

b. Ensure that handling of incident information is in accordance with all data sensitivity requirements.

c. Support information security investigations as appropriate.

3.4.5.6 The ISSO shall ensure effective and timely reporting of all suspected or confirmed security incidents.

3.4.5.7 The NASA User shall report immediately all suspected, or actual, information security incidents to the SOC as outlined in the incident response and management handbook(s).

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

3.5 Maintenance (MA)

3.5.1 The Maintenance control family relates to the continuous upkeep of information and information systems. In general, maintenance controls are very system specific, and are typically performed based upon vendor recommendations. Many variable factors are considered when making the appropriate maintenance decisions for a system. The business impact, cost, and likelihood of equipment failure, the cost of the maintenance agreement, and the availability of spare equipment can all influence the application of specific Maintenance controls.

3.5.2 NASA recognizes that decisions regarding system specific maintenance requirements are best managed at the information system level, where the specific risks are well understood. However, all Maintenance controls at the information system level must be based on a thorough risk analysis, and accepted risks must be well documented.

3.5.3 Maintenance procedures shall be governed by ITS-HBK-2810.10, Maintenance.

3.5.4 Maintenance Policy

3.5.4.1 The ISO shall:

a. Develop, maintain, and execute a risk-based maintenance policy and procedures.

b. Adhere to change control and configuration management processes throughout the life cycle of their information systems.

c. Maintain oversight of those authorized to perform maintenance on the components of their information system.

3.6 Media Protection (MP)

3.6.1 The Media Protection control family relates to the secure use of information storage media. Storage media can take one of two forms - digital or non-digital. Non-digital media typically consists of paper, film, microfilm, microfiche, etc. Digital media is comprised of mobile computing devices, laptops, personal digital assistants (PDA), "smart phones," and removable storage devices such as USB drives, flash drives, writeable compact discs (CD), and digital video discs (DVD), memory cards, external hard drives, storage cards, diskettes, magnetic tapes, external/removable hard drives, or any electronic device that can be used to copy, save, store and/or move data from one system to another.

3.6.2 The objective of the control family is to prevent or mitigate data loss and/or unauthorized access to NASA information and information systems, due to a failure to secure media, or a failure to sanitize media prior to reuse or disposal.

3.6.3 NASA follows the requirements of FIPS 140, Security Requirements for Cryptographic Modules.

3.6.4 NASA utilizes the guidelines of NIST SP 800-88, Guidelines for Media Sanitization; and NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

3.6.5 Media Protection procedures shall be governed by ITS-HBK-2810.11, Media Protection.

a. Special considerations for the use of mobile devices during domestic and international travel are

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

discussed and governed by NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

3.6.6 Media Protection Policy

3.6.6.1 The Center CISO shall:

a. Ensure, in coordination with the Center Security Office, that sufficient equipment or services are available to facilitate media sanitization.

b. Ensure that portable and removable digital media devices are guarded using encryption solutions which are compliant with federal encryption algorithm standards and NIST guidance, and are in accordance with NASA requirements regarding the protection of sensitive information.

3.6.6.2 The OCSO shall be responsible for the protection and sanitization of media for their organization. This includes the protection of data at rest.

3.6.6.3 The ISO shall be responsible for the protection and sanitization of media for their information system. This includes the protection of data at rest.

3.6.6.4 The NASA User shall mitigate the risks of data loss by securing and protecting media under their control, and the information contained on/within those devices, through the use of encryption, access restriction, and/or sanitization.

3.6.6.5 The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the implementation of media protection security controls.

3.7 Physical and Environmental Protection (PE)

3.7.1 The Physical and Environmental Protection control family relates to the activities and requirements surrounding the development, implementation, and maintenance of physical access authorizations and controls (e.g., key and security badge distribution, visitor management, and related record keeping), and the protection, proofing, and regulation of facilities. NASA protects its facilities and the essential utilities and infrastructure which support those facilities (e.g., door locks, backup power and lighting, emergency plumbing shutoff switches, and fire suppression systems), and also provides appropriate environmental controls for those facilities (e.g., temperature regulation, humidity monitoring). Members of the NASA community are responsible for being aware of, and diligently exercising all facility safety and security procedures.

3.7.2 Physical and Environmental Protection procedures shall be governed by NPR 1600.1, NASA Security Program Procedural Requirements ; NPR 1620.2, Physical Security Vulnerability Risk Assessments ; NPR 1620.3, Physical Security Requirements for NASA Facilities and Property ; NPR 8820, Facility Project Requirements ; NPR 8831.2, Facilities Maintenance and Operations Management ; and ITS-HBK-2810.12, Physical and Environmental Protection.

3.7.3 Physical and Environmental Policy

3.7.3.1 The Center CIO shall work with the Center Chief of Security, and/or the Center Facilities organization to ensure physical and environmental controls are met for the information systems at their Centers.

3.7.3.2 The ISO shall:

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

a. Approve personnel need to access secured/restricted physical information system facilities and locations.

b. Establish and maintain a list of all personnel authorized to access secured/restricted physical information system facilities and locations.

c. Validate physical and environmental security controls and monitoring capabilities.

3.7.3.3 The Center Chief of Security under the policy guidance of Assistant Administrator of the Office of Protective Services shall:

a. Ensure the implementation of physical and environmental security controls.

b. Ensure the capability to monitor physical and environmental security controls.

3.8 Personnel Security (PS)

3.8.1 The Personnel Security control family relates to the security activities that surround various facets of the employment life cycle (i.e., initial employee screening, position categorization, authority delegation, sanctioning, transfers, and termination). Personnel Security applies to both direct employees of the Agency as well as contracted personnel, and service bureaus.

3.8.2 Personnel Security procedures shall be governed by NPD 1600.2, NASA Security Policy; NPD 1600.3, Policy on Prevention of and Response to Workplace Violence ; NPR 2841.1, Identity, Credential, and Access Management Services ; and ITS-HBK-2810.13, Personnel Security.

3.8.3 Personnel Security Policy

3.8.3.1 The SAISO shall ensure that all offices are aware of requirements and expectations related to personnel security.

3.8.3.2 The Center CISO shall confirm that all personnel adhere to the limits of their delegated authority, and act accordingly to address deviations.

3.8.3.3 The ISO shall:

a. Ensure that all personnel are screened prior to the provision of access to information and information systems.

b. Ensure that access to secured resources are managed or terminated following the transfer or termination of personnel.

3.8.3.4 The Center Chief of Security under the policy guidance of the Assistant Administrator of Office of Protective Services shall ensure the implementation of personnel security controls.

3.9 System and Information Integrity (SI)

3.9.1 The System and Information Integrity control family relates to the prevention and detection of improper modification or destruction of information or an information system. The control family also includes ensuring the non-repudiation and authenticity of information, as well as flaw remediation (e.g., patching vulnerable software), malicious code prevention (e.g., anti-virus

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

software), and monitoring of attempts to subvert integrity (e.g., an intrusion detection system).

3.9.2 System and Information Integrity procedures shall be governed by ITS-HBK-2810.14, System and Information Integrity.

3.9.3 System and Information Integrity Policy

3.9.3.1 The SAISO shall:

a. Establish resources for the management of vulnerability, flaw remediation, and information system monitoring.

b. Ensure the proper handling of vulnerability/patch advisories, including the aggregation of such information from sources both internal and external to the Agency and the Federal government, as well as the wide distribution of such information.

c. Ensure that the appropriate resources exist to comply with NASA requirements regarding System and Information Integrity including capabilities to detect and prevent the compromise of integrity by known threats (e.g., anti-virus software, block lists) and suspected threats (e.g., automated spam classification and filtering).

3.9.3.2 The Center CISO shall facilitate the implementation of NASA flaw remediation policies and procedures at their Center.

3.9.3.3 The ISO shall:

a. Ensure that all information system components are identified and documented.

b. Ensure the completion of flaw remediation activities, and document and communicate residual risks as necessary.

c. Ensure the implementation of malicious code protections on their information systems.

d. Ensure that information system security functions are tested in accordance with requirements, and that the frequency and processes related to the tests are formally documented.

Chapter 4 - Technical Controls

4.1 Access Control (AC)

4.1.1 The Access Control security control family relates to the ability of NASA to permit or deny access to computer systems, system locations and system information based on a user's assigned duties. The control family encompasses the management of unique account identifiers (IDs), passwords, physical access, badges and tokens, and user permissions to ensure the proper level of system access.

4.1.2 NASA follows the requirements of HSPD-12, Policies for a Common Identification Standard of Federal Employees and Contractors.

4.1.3 NASA utilizes the guidelines of NIST SP 800-46, Guide to Enterprise Telework and Remote Access Security; NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

4.1.4 Access Controls procedures shall be governed by NPR 2841.1, Identity, Credential, and Access Management Services; ITS-HBK-2810.15, Access Control; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.1.5 Access Control Policy

4.1.5.1 The SAISO shall:

a. Ensure dissemination of the NASA appropriate use policy statement, based on NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology, and the NASA warning banner.

b. Ensure that the NASA warning disclaimer requirements for internal systems are met through the display of the appropriate use and warning banner statements as follows:

1. All computers and applications that are owned by or operated on behalf of NASA and require user authentication for access must display and require acknowledgement of the following NASA warning banner prior to logging on to a NASA system:

This US Government computer is for authorized users only. By accessing this system you are consenting to complete monitoring with no expectation of privacy. Unauthorized access or use may subject you to disciplinary action and criminal prosecution.

2. The following disclaimer is a policy statement which requires concurrence from all users of NASA information systems:

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

4.1.5.2 The ISO shall:

a. Ensure account management capabilities (e.g., account creation, privilege configuration, maintenance, and deletion) are in place for their information systems.

b. Ensure that accounts for their information systems are administered in a way which provides separation of duties, avoids potential conflicts of interest, and grants NASA users the least privilege necessary to execute their respective duties.

c. Manage, in collaboration with the IO, access to the information system, and with which privileges users will be authorized.

d. Ensure the appropriate use and warning banner is displayed by their information system.

e. Establish documented rules for appropriate use and protection of information (e.g., rules of behavior).

4.1.5.3 The IO shall collaborate with the ISO to manage access to the information system, and with which privileges users will be empowered.

4.1.5.4The NASA User shall comply with all appropriate use policies.

4.2 Audit and Accountability (AU)

4.2.1 The Audit and Accountability control family relates to the documentation and management of events that occur on or to information system components. Generally, the controls help to answer the questions of "who," "what," "where," "when," and sometimes "how" revolving around various types of information system activities and events (i.e., who logged into a given machine, when, and from where, etc.?). Such audit trails are used for individual accountability, intrusion detection, and problem identification.

4.2.2 Such details are stored in logs which are used to produce useful, actionable information by applying data analysis techniques to detect anomalous trends and patterns that may be cause for concern. The logs can be used both retroactively to determine the causes of an adverse event, and proactively to detect and take action to avoid an imminent adverse event.

4.2.3 Audit and Accountability procedures shall be governed by NPR 1441.1, NASA Records and Retention Schedule; and ITS-HBK-2810.16, Audit and Accountability.

4.2.4 Audit and Accountability Policy

4.2.4.1 The NASA CIO shall e nsure the development and maintenance of a capability for the aggregation of NASA-wide information system logs.

4.2.4.2 The SAISO shall:

a. Ensure that NASA maintains Agency information system record retention policies for logs, and minimum auditable events.

b. Ensure the development and maintenance of log security auditing capabilities for NASA information system logs.

4.2.4.3 The ISO shall:

a. Ensure and maintain auditing capabilities for their information system components with consideration given to storage capacity.

b. Determine the appropriate priorities for audit log events, analysis, and responses. The manner of log collection, extent of the audited events, specific data per event, analysis of the event, and retention times of the audit data will be dependent upon risk levels and the technical capabilities of the components.

c. Ensure audit logs are strongly controlled, and protected from modification and unauthorized disclosure. This protection should exist throughout the life cycle of the log entry, through creation, transmission, aggregation, reduction, analysis, storage, and disposal.

4.3 Identification and Authentication (IA)

4.3.1 The Identification and Authentication control family relates to the activities and provisions which ensure the identity of a given entity requesting access to NASA resources (e.g., a person logging in to a computer, or a laptop computer connecting to a wireless network). The controls address the creation, management, usage, and protection of identities (e.g., usernames) and authenticators (e.g., passwords, smart cards, and tokens).

4.3.2 NASA follows the requirements of HSPD-12, Policies for a Common Identification Standard of Federal Employees and Contractors; OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies; OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors; FIPS 140, Security Requirements for Cryptographic Modules; and FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

4.3.3 NASA utilizes the guidelines of NIST SP 800-63, Electronic Authentication Guideline.

4.3.4 Identification and Authentication procedures shall be governed by NPR 1600.1, NASA Security Program Procedural Requirements; NPR 2841.1, Identity, Credential, and Access Management Services; ITS-HBK-2810.17, Identification and Authentication ; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.3.5 Identification and Authentication Policy

4.3.5.1 The NASA CIO shall provide a NASA-wide framework for identity and authentication management.

4.3.5.2 The ISO shall ensure that applications leverage the Agency identification and authentication framework.

4.3.5.3 The NASA User shall protect identification and authentication information from unauthorized disclosure.

4.3.5.4 The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the distribution and management of physical authenticators (e.g., smart cards, and tokens).

4.4 System and Communications Protection (SC)

4.4.1 The System and Communication control family relates to the protection of confidentiality, integrity, and availability of NASA information systems and NASA information as it flows between communications networks. The control family ensures the establishment of an effective physical and logical network security perimeter and provides guidance for best protecting information as it moves both within the security perimeter and as it moves to and from other networks outside the security perimeter such as the Internet.

4.4.2 NASA follows the requirements of X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework; and FIPS 140, Security Requirements for Cryptographic Modules.

4.4.3 System and Communication procedures shall be governed by ITS-HBK-2810.18, System and Communication; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.4.4 System and Communications Policy

4.4.4.1 The NASA CIO shall:

a. Ensure that NASA develops, implements, and maintains Agency common system and communications infrastructure.

b. Ensure the development and maintenance of a NASA-wide cryptographic key management framework.

4.4.4.2 The Center CIO shall:

a. Ensure the integration of software and hardware necessary to support system and communications requirements at their Center.

b. Provision Center-level boundary protection activities for systems which share a common infrastructure and/or services.

4.4.4.3 The ISO shall ensure the implementation of shared resource policies, denial of service protections, boundary protection, and transmission integrity and confidentiality.

Appendix A: Definitions

	Term	Definition
A.1	**Authorization to Operate**	The formal acceptance, by an Authorizing Official, that the security of an information system's operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system's confidentiality, integrity, and availability.
A.2	**Boundary Protection**	The security safeguards or countermeasures in place on an information system's logical and physical perimeters.
A.3	**Common Control**	A security safeguard or countermeasure which may be designed, implemented, and assessed at a level which encompasses one or more information systems.
A.4	**Continuous Monitoring**	The ongoing, and often high-frequency, assessment of an information system's security posture usually enabled through the use of automated tools which measure the effectiveness of specific security controls.
A.5	**External Information System**	Any information system which is either owned, or operated by an organization other than NASA, and which processes, maintains, uses, shares, disseminates, or dispositions NASA data.
A.6	**Handbook**	An Agency-level, SAISO-approved document which prescribes the best practices, policies, and procedures regarding various information system security topics.
A.7	**Hybrid Control**	A security safeguard or countermeasure which requires system-specific consideration and may also be partially designed, implemented, and assessed at a level which encompasses one or more information systems.
A.8	**Incident**	Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality
A.9	**Information Security**	The protection of an information system's confidentiality, integrity, and availability.
A.10	**Information System**	A discrete set of resources designed and implemented for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
A.11	**Internal Information System**	Any information system which is owned and operated by NASA.
A.12	**Least Privilege**	The concept of limiting the flexibility of use an information system user or component has, to the degree necessary to perform a specified role.
A.13	**Management Control**	The collection of supervisory NIST SP 800-53 controls dedicated to information system security.
A.14	**NASA Center**	Any of the collection of facilities and installations designated by NASA, and usually grouped by function (e.g., research, construction, administration).
A.15	**NASA Information**	Any data which is collected, generated, maintained, or controlled on behalf of the Agency.
A.16	**NASA User**	Any explicitly authorized patron of a NASA information system.
A.17	**Near Real-Time (Risk Assessment)**	An analysis of an information system's security posture which closely reflects the immediate state of the system.
A.18	**Non-Digital Media**	Any non-electronic information storage medium (e.g., paper).
A.19	**Ongoing Authorizations**	The continuous acceptance of an information system's operation based on a real-time understanding of the system's security posture.
A.20	**Operational Control**	The collection of strategic NIST SP 800-53 controls dedicated to information system security.
A.21	**Organizationally-Defined Values**	Those details of certain security controls which are meant to be determined by the managing entity. Typically, a memo delivered annually by the OCIO which defines specific details of a security controls implementation.
A.22	**Risk Assessment**	The value-based analysis of an information system's security posture.
A.23	**Risk Management**	A framework defined by NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
A.24	**Security Posture**	The overall state of an information system's confidentiality, integrity, and availability in the face of an ever-changing risk landscape.
A.25	**Technical Control**	The collection of tactical NIST SP 800-53 controls dedicated to information system security.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Appendix B: Acronyms

	Term	Definition
B.1	**AC**	Access Control
B.2	**AO**	Authorizing Official
B.3	**AODR**	Authorizing Official Designated Representative
B.4	**AT**	Awareness and Training
B.5	**ATO**	Authorization to Operate
B.6	**AU**	Audit and Accountability
B.7	**CA**	Certification Authority
B.8	**CD**	Compact Disc
B.9	**C.F.R.**	Code of Federal Regulations
B.10	**CIO**	Chief Information Officer
B.11	**CISO**	Chief Information Security Officer
B.12	**CM**	Configuration Management
B.13	**CNSI**	Classified National Security Information
B.14	**COOP**	Continuity of Operations
B.15	**CP**	Contingency Plan
B.16	**CT**	Counterterrorism
B.17	**DVD**	Digital Video Disc
B.18	**e .g.**	For Example
B.19	**ESIGN**	Electronic Signatures in Global and National Commerce
B.20	**Etc.**	Et Cetera
B.21	**Exec.**	Executive
B.22	**FAR**	Federal Acquisition Regulations
B.23	**FDCC**	Federal Desktop Core Configuration
B.24	**FIPS**	Federal Information Processing Standards
B.25	**FISCAM**	Federal Information System Controls Audit Manual
B.26	**FISMA**	Federal Information Security Management Act
B.27	**GAO**	Government Accounting Office
B.28	**GOCO**	Government Owned, Contractor Operated
B.29	**HSPD**	Homeland Security Presidential Directive
B.30	**IA**	Identification and Authorization
B.31	**ICAM**	Identity, Credential, and Access Management
B.32	**ID**	Identification
B.33	**IEEE**	Institute of Electrical and Electronic Engineers
B.34	**IR**	Incident Response and Management
B.35	**IO**	Information Owner

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

B.36	**ISA**	Interconnection Security Agreement
B.37	**ISO**	Information System Owner
B.38	**ISSO**	Information System Security Officer
B.39	**IT**	Information Technology
B.40	**ITS-HBK**	Information Technology Security Handbook
B.41	**ITSAB**	Information Technology Security Advisory Board
B.42	**JPL**	Jet Propulsion Laboratory
B.43	**MA**	Media Access
B.44	**MOA**	Memorandum of Agreement
B.45	**MOU**	Memorandum of Understanding
B.46	**MP**	Media Protection
B.47	**NASA**	National Aeronautics and Space Administration
B.48	**NIST**	National Institute of Standards and Technology
B.49	**NITR**	NASA Information Technology Requirement
B.50	**NPD**	NASA Policy Directive
B.51	**NPR**	NASA Procedural Requirement
B.52	**NTISS**	National Telecommunications and Information System Security
B.53	**OCIO**	Office of the Chief Information Officer
B.54	**OCSO**	Organizational Computer Security Official
B.55	**OIG**	Office of the Inspector General
B.56	**OMB**	Office of Management and Budget
B.57	**OPS**	Office of Protective Services
B.58	**PDA**	Personal Digital Assistant
B.59	**PE**	Physical and Environmental Protection
B.60	**PIA**	Privacy Impact Assessment
B.61	**PM**	Program/ Project Manager
B.62	**POA &M**	Plan of Action and Milestones
B.63	**PL**	Planning
B.64	**P ub. L./ P.L.**	Public Law
B.65	**PS**	Protective Services
B.66	**RA**	Registration Authorities
B.67	**RMF**	Risk Management Framework
B.68	**SA**	System and Services Acquisition
B.69	**SAISO**	Senior Agency Information Security Officer
B.70	**SBU**	Sensitive But Unclassified
B.71	**SC**	System and Communications Protection
B.72	**SI**	System and Information Integrity
B.73	**SOC**	Security Operations Center
B.74	**SP**	Special Publication

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

B.75	**SSP**	System Security Plan
B.76	**USA PATRIOT**	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
B.77	**USB**	Universal Serial Bus
B.78	**U.S.C.**	United States Code
B.79	**USGCB**	United States Government Configuration Baseline
B.80	**VPN**	Virtual Private Network

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Appendix C: Responsibility Cross-Walk

	NASA Administrator	NASA CIO	NASA Center Director	Center CIO	SAISO	Center CISO	OCSO	AO	AODR	ISO	IO	ISSO	NASA User
Overarching *(Chapter 1)*	2.3.1	2.3.2	2.3.3	2.3.4	2.3.5	2.3.6	2.3.7	2.3.8	2.3.9	2.3.10	2.3.11	2.3.12	2.3.13
1 – PM		2.1.3.1			2.1.3.2								
2 – CA *(See HBK 2810-02)*		2.2.3.1			2.2.3.2	2.2.3.3	2.2.3.4	2.2.3.5		2.2.3.6	2.2.3.7		
3 – PL *(See HBK 2810-03)*					2.3.4.1		2.3.4.2	2.3.4.3		2.3.4.4			
4 – RA *(See HBK 2810-04)*					2.4.5.1	2.4.5.2		2.4.5.3		2.4.5.4			
5 – SA *(See HBK 2810-05)*					2.5.3.1					2.5.3.2	2.5.3.3	2.5.3.4	
6 – AT *(See HBK 2810-06)*		3.1.3.1			3.1.3.2	3.1.3.3	3.1.3.4			3.1.3.5			3.1.3.6
7 – CM *(See HBK 2810-07)*					3.2.4.1					3.2.4.2		3.2.4.3	
8 – CP *(See HBK 2810-08)*				3.3.5.1	3.3.5.2	3.3.5.3				3.3.5.4			
9 – IR *(See HBK 2810-09)*		3.4.5.1		3.4.5.2	3.4.5.3	3.4.5.4				3.4.5.5		3.4.5.6	3.4.5.7
10 – MA *(See HBK 2810-10)*										3.5.4.1			
11 – MP *(See HBK 2810-11)*						3.6.6.1	3.6.6.2			3.6.6.3			3.6.6.4
12 – PE *(See HBK 2810-12)*				3.7.3.1						3.7.3.2			

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

13 – PS ***(See HBK 2810-13)***					3.8.3.1	3.8.3.2				3.8.3.3			
14 – SI ***(See HBK 2810-14)***					3.9.3.1	3.9.3.2				3.9.3.3			
15 – AC ***(See HBK 2810-15)***					4.1.5.1					4.1.5.2	4.1.5.3		4.1.5.4
16 – AU ***(See HBK 2810-16)***		4.2.4.1			4.2.4.2					4.2.4.3			
17 – IA ***(See HBK 2810-17)***		4.3.5.1								4.3.5.2			4.3.5.3
18 – SC ***(See HBK 2810-18)***		4.4.4.1		4.4.4.2						4.4.4.3			

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Appendix D: Role Definitions

	Role	Definition
D.1	**NASA CIO**	The principal advisor to the Administrator, and other senior officials on matters pertaining to information technology.
D.2	**Center CIO**	The principal advisor the NASA CIO, and senior Center officials on matters pertaining to information technology.
D.3	**SAISO**	The principal advisor to the NASA CIO, and other senior officials on matters pertaining to information security.
D.4	**Center CISO**	The principal advisor to the SAISO, Center CIO, and senior Center officials on matters pertaining to information security. This role was previously referred to as the Information Technology Security Manager.
D.5	**OCSO**	The principal advisor to the Center CISO on matters pertaining to organizational information security.
D.6	**AO**	The Agency official who authorizes the use of information systems, and is accountable for all accepted risks associated with that authorization.
D.7	**AODR**	The delegate of the AO.
D.8	**ISO**	The principal advisor to the Center CISO on matters pertaining to specific information systems.
D.9	**IO**	The principal advisor to the ISO on matters pertaining to data and information which is resident on specific information systems.
D.10	**ISSO**	The principal advisor to the ISO on matters pertaining to the security of specific information systems.
D.11	**NASA User**	Any explicitly authorized patron of a NASA information system.

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

Appendix E: References

E.1 40 U.S.C. § 11101, et seq., Chapter 808 of Pub. L 104-208, the Clinger-Cohen Act of 1996

E.2 44 U.S.C. § 3535, Federal Information Security Management Act (FISMA) of 2002

E.3 FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, 2006

E.4 OMB Circular A-11, Preparation, Submission and Execution of the Budget, July 2004

E.5 OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, November 2000

E.6 OMB Memorandum M-00-13, Privacy Policies, and Data Collection on Federal Web Sites, June 22, 2000

E.7 OMB Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, August 2003

E.8 OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003

E.9 OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003

E.10 OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—

E.11 OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006

E.12 OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 2006

E.13 OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007

E.14 OMB Memorandum M-08-21, FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 2008

E.15 National Telecommunications and Information System Security (NTISS) 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems, June 17, 1982

E.16 NTISS 100, National Policy on Application of Communications Security to Command Destruct Systems, February 17, 1988

E.17 Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, December 2003

E.18 GAO-09-232G, Federal Information System Controls Audit Manual (FISCAM)

E.19 NPD 1382.17, NASA Privacy Policy

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.

E.20 NPD 1440.6, NASA Records Management

E.21 NPD 1600.2, NASA Security Policy

E.22 NPD 7100.8, Protection of Human Research Subjects

E.23 NPD 7120.4, NASA Engineering and Program/Project Management Policy

E.24 NPR 1660.1, Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirement

E.25 NPR 2190.1, NASA Export Control Program

E.26 NPR 2800.1, Managing Information Technology

E.27 NPR 2830.1, NASA Enterprise Architecture Procedures

E.28 NPR 7100.1, Protection of Human Research Subjects

E.29 NPR 7120.5, NASA Space Flight Program and Project Management Requirements

E.30 NPR 7120.6, Lessons Learned Process

E.31 NPR 7150.2, NASA Software Engineering Requirements

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.