NASA
Procedural
Requirements

NPR 2810.1
Effective Date: January 3, 2022
Expiration Date: January 3 2027

COMPLIANCE IS MANDATORY FOR ALL NASA EMPLOYEES

Security of Information and Information Systems

Responsible Office: Office of the Chief Information Officer

Table of Contents

Preface

P.1 Purpose
P.2 Applicability
P.3 Authority
P.4 Applicable Documents and Forms
P.5 Measurement/Verification
P.6 Cancellation

Chapter 1. Introduction

1.1 Introduction
1.2 Roles and Responsibilities

Chapter 2. Identify Function

2.1 Asset Management
2.2 Business Environment
2.3 Governance
2.4 Risk Assessment
2.5 Risk Management Strategy
2.6 Supply Chain Risk Management

Chapter 3. Protect Function

3.1 Identity Management and Access Control
3.2 Awareness and Training

3.3 Data Security
3.4 Information Protection Processes and Procedures
3.5 Maintenance
3.6 Protective Technology

Chapter 4. Detect Function

4.1 Anomalies and Events
4.2 Security Continuous Monitoring
4.3 Detection Processes

Chapter 5. Respond Function

5.1 Response Planning
5.2 Communications
5.3 Analysis
5.4 Mitigation
5.5 Improvements

Chapter 6. Recover Function

6.1 Recovery Planning
6.2 Improvements
6.3 Communications

Appendix A Definitions
Appendix B Acronyms
Appendix C Requirements Matrices
Appendix D References
Appendix E Requirements Matrix with respect to system lifecycle

Preface

P.1 Purpose

a. This directive establishes the information security requirements for the 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, including operational technology systems.

b. This directive identifies information security policies, procedures, and practices that are related to NASA's mission, and consistent with federal laws, executive orders, directives, policies, and regulations.

c. This directive aligns roles and responsibilities of information technology (IT) security personnel to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy and NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.

d. This directive serves as a reference to the NASA community regarding specific information security roles and responsibilities, and it provides resources where more detailed information may be found.

e. This directive implements cybersecurity policy best practices and guidance, particularly those outlined by the NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations, NIST SP 800-37, NIST SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, NIST 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems – A Systems Security Engineering Approach, and NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, referenced NASA policy documents, specifications, and standards, and mandated by Federal Information Processing Standards (FIPS) across all corporate, project, and mission elements (ground and flight systems).

P.2 Applicability

a. This directive applies to NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers.

(1) For purposes of this directive, NASA Headquarters is treated as a Center. Further, all roles and responsibilities of a Center Chief Information Officer (CIO) apply to NASA Headquarters CIO and all stipulated Center requirements apply to NASA Headquarters.

b. This directive applies to contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the contracts, grants, or agreements.

c. This directive applies to all unclassified NASA information and NASA information systems, including those that are contracted out, outsourced to, or operated by:

(1) Government owned, contractor operated (GOCO) facilities;

(2) partners under the Space Act;

(3) partners under the Commercial Space Act of 1997;

(4) partners under cooperative agreements; or

(5) commercial or university facilities.

d. This directive does not apply to information systems that do not process NASA information, and are merely incidental to a contract (e.g., a contractor's payroll and personnel management system).

(1) In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms: “may” or “can” denote discretionary privilege or permission, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive material.

e. This directive does not apply to Classified National Security Information (CNSI). CNSI is the responsibility of the Office of Protective Services (OPS) and is covered under CNSI policy and requirements contained in NASA Procedural Requirement (NPR) 1600.2, NASA Classified National Security Information (CNSI) and NPR 1600.1, NASA Security Program Procedural Requirements.

f. This directive applies to all NASA users of information systems (e.g., civil servants and contractors) when supporting Agency projects, programs, and missions.

g. In this directive all document citations are assumed to be the latest version unless otherwise noted.

P.3 Authority

a. Freedom of Information Act, 5 U.S.C. § 552, et seq.

b. Privacy Act of 1974, 5 U.S.C. § 552a.

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

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

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

f. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101 et seq.

g. Federal Information Technology Acquisition Reform Act (FITARA) of 2014, 40 U.S.C. § 11319 et seq.

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

i. Paperwork Reduction Act of 1995, 44 U.S.C. § 3501, et seq.

j. Federal Information Security Management Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq.

k. Export Control Reform Act of 2018, 50 U.S.C. 4801-4852.

l. National Aeronautics and Space Act, 51 U.S.C. § 20113(e).

m. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, E.O. 13800, 82 FR 22391 (2017).

n. Availability of Agency Records to Members of the Public, 14 Code of Federal Regulations (CFR) pt. 1206.

o. Export Administration Regulations, 15 CFR pts. 730-774.

p. International Traffic in Arms Regulations, 22 CFR pts. 120-130.

q. 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.

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

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

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

u. HSPD-20, National Continuity Policy.

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

P.4 Applicable Documents and Forms

a. NASA Federal Acquisition Regulations (FAR) Supplement, 48 CFR Chapter 18.

b. NPD 1000.0, NASA Governance and Strategic Management Handbook

c. NPD 1000.3, The NASA Organization

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

e. NPD 2810.1, NASA Information Security Policy.

f. NASA Records Retention Schedule No 1441.1 (updated) May 18, 2020.

g. NPR 1600.1, NASA Security Program Procedural Requirements.

h. NPR 1600.2, NASA Classified National Security Information (CNSI).

i. NPR 2841.1, Identity, Credential, and Access Management.

j. NPR 4200.1, NASA Equipment Management Procedural Requirements.

k. NPR 8000.4, Agency Risk Management Procedural Requirements.

l. NASA Advisory Implementing Instruction (NAII) 1050.3, NASA Partnership Guide.

m. NASA-STD-1006, Space System Protection Standard.

n. NASA-SPEC-2600, Enumeration of ASCS Cybersecurity Requirements.

o. NIST Special Publication (SP) 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

p. NIST SP 800-171, Rev 2 Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations.

q. NIST SP 800-46, Guide to Enterprise Telework and Remote Access, and Bring Your Own Device (BYOD) Security.

r. NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

s. NIST SP 800-60, Volumes 1 and 2, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices.

t. NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security and Organizations.

u. NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems – A Systems Security Engineering Approach.

v. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

w. ITS-HBK-2810.11-2B Media Protection and Sanitization.

x. Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-02 Securing High Value Assets.

P.5 Measurement/Verification

a. Federal regulatory and NASA requirements drive the obligation to measure performance and reduce cost. These measurements will be based upon NASA's goals and objectives and be designed to provide substantive justification for decision-making. The measures will be used to measure the effectiveness of the information security program, policies, and requirements.

b. The NIST Cybersecurity Framework is the fundamental basis of such measurement.

c. The Senior Agency Information Security Officer (SAISO) will provide assessments or audit of the application of this directive. Assessments and audits will consist of reporting from the Centers, including information collected for the satisfaction of Office of Management and Budget (OMB) and FISMA reporting requirements.

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

P.6 Cancellation

a. NPR 2810.1A, Security of Information Technology, dated May 16, 2006.

Chapter 1. Introduction

1.1 Introduction

1.1.1 Structure

1.1.1.1 This directive establishes the information security requirements and responsibilities for NASA, relative to the policy set forth in NPD 2810.1, NASA Information Security Policy. This directive 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, memoranda).

1.1.1.2 This directive is organized into six chapters: (1) Introduction; (2) Identify; (3) Protect; (4) Detect; (5) Respond; and (6) Recover.

a. The chapters in this directive align to the functional areas of version 1.1 of the NIST Cybersecurity Framework (CSF).

b. Each chapter defines the overall intent of the functional area and the roles and responsibilities specific to the area. Each chapter provides references to where more detailed requirements, procedures, and information may be found.

1.1.2 Approach

1.1.2.1 NASA's SAISO establishes the Agency's Cybersecurity and Privacy 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 consistent with this directive and more in-depth policy documents authorized by this directive.

1.1.2.2 NASA's approach to information security is grounded in risk management. Just as a solid understanding of risk management principles is essential to the success of NASA's space and aeronautics Missions, a solid understanding of these principles is essential to the protection of NASA information and information systems.

1.1.3 Legal Framework

1.1.3.1 Existing laws, regulations, and guidance govern NASA's implementation of an information security program.

a. The primary statute governing information security is FISMA, which defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

b. This directive establishes how NASA implements the requirements of FISMA as they relate to NASA information and information systems.

c. The Clinger-Cohen Act states that the NIST FIPS are "compulsory and binding" 40 U.S.C. § 11331(b)(1)(C). FISMA also advocates that information 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," Federal Agency Responsibilities, 44 U.S.C. § 3554(b)(1). FISMA provides flexibility regarding the application of information security controls.

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

1.2 Roles and Responsibilities

1.2.1 Overview

1.2.1.1 The following are overarching roles and responsibilities related to the NASA Cybersecurity and Privacy Program. Specific roles and responsibilities, as related to information security controls, are referenced throughout the remainder of this directive in their respective chapters. Additional responsibilities may be defined in in-depth policy documents authorized by this directive.

1.2.1.2 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.

1.2.1.3 For the Jet Propulsion Laboratory (JPL), the Agency CIO will designate the roles allocated for the United States federal government employees.

1.2.2 NASA Management Roles

1.2.2.1 The roles and responsibilities of NASA management are defined in NPD 1000.0, NASA Governance and Strategic Management Handbook, and further outlined in NPD 1000.3, The NASA Organization. The key roles and responsibilities specific to information security are summarized as follows:

1.2.2.2 The NASA Administrator shall:

a. Ensure the security of NASA's information and information systems.

b. Ensure that NASA implements the NIST Cybersecurity Framework.

1.2.2.3 The NASA CIO provides leadership, planning, policy direction, and oversight for the management of NASA information and information systems. The NASA CIO shall:

a. Ensure confidentiality, integrity, and availability of all NASA's information assets throughout the system life cycle.

b. Ensure all NASA IT is in compliance with federal and NASA Cybersecurity and Privacy Program requirements.

c. Commission suitable governance bodies.

d. Evaluate and approve the designation of Authorizing Officials (AO).

e. Advise senior NASA officials concerning their information security responsibilities.

f. Ensure the NASA enterprise architecture integrates information security considerations into the strategic, capital, and investment planning process.

g. Encourage the maximum reuse and sharing of information security-related information throughout the NASA community.

h. Develop, implement, and maintain a Controlled Unclassified Information (CUI) program which is managed in accordance with Executive Order (E.O.) 13556, Controlled Unclassified Information, and Controlled Unclassified Information, 32 CFR, pt. 2002.

i. Be an employee of the United States Federal Government.

1.2.2.4 Officials in charge of Mission Directorates and Mission Support Offices shall:

a. Appoint an information security point of contact to represent the mission on Agency programmatic strategic cybersecurity initiatives and serve as a voting member of suitable governance bodies.

b. Ensure that resources are allocated to address information and information system security requirements developed under this directive for their information systems.

c. Ensure that their respective organizations, including missions, programs, projects, and institutions under their purview, comply with this directive, ensuring Operational Technology is also compliant.

d. Ensure that secure software development is being practiced for NASA projects per NPR 7150.2, NASA Software Engineering Requirements.

e. Ensure that secure system development is being practiced for NASA projects per NASA specifications and standards, including NASA-STD-1006, and the NASA Cybersecurity Requirements Technical Specification.

1.2.2.5 The Center Directors and the Director for Headquarters Operations shall:

a. With concurrence from the SAISO and the Center’s CIO, designate a Center Chief Information Security Officer (CISO) in writing.

b. Ensure the Center CISO has adequate staff, resources, budget, and authority to implement information security programs at their Center.

1.2.3 Information Security Roles

1.2.3.1 In addition, the following offices and roles support the development and execution of information security policy are listed in the following paragraph.

1.2.3.2 A Center CIO shall:

a. If they apply, execute the responsibilities, comparable to those of the NASA CIO, at the Center level.

b. Execute the responsibilities, comparable to those of the NASA CIO, with respect to NASA facilities and systems not located at a Center as designated by the CIO.

c. If the Center CIO assigns an Organizational Computer Security Official (OCSO) per section 1.2.3.3, designate Center-specific OCSO responsibilities, and any necessary interfaces with the Center CISO, in a Center-level formal policy.

d. Be an employee of the United States Federal Government.

1.2.3.3 A Center CIO may optionally assign OCSOs to facilitate the implementation and oversight of information security within their organization.

1.2.3.4 The SAISO shall:

a. Carry out the responsibilities delegated from the NASA CIO under FISMA (as provided for by 44 U.S.C § 3554(a)(3)(A)), as well as federal and NASA cybersecurity and privacy program requirements.

b. Establish and maintain an office with the mission and resources to ensure compliance with federal and NASA Cybersecurity and Privacy Program requirements.

c. Manage the NASA Cybersecurity and Privacy Program.

d. Keep the NASA Cybersecurity and Privacy Program current with changes in the information security environment and with changes in federal policy and guidelines.

e. Ensure that information security control assessments, authorizations, and OMB and FISMA reporting directives are completed across the Agency in a timely and cost-effective manner.

f. Serve as the NASA CIO's primary liaison with Center CISOs, AOs, Information System Owners (ISOs), and Information System Security Officers (ISSOs).

g. Oversee and arbitrate conflict resolution, relative to information security concerns, for all NASA-wide information systems.

h. Ensure the planning of a framework for the use and adoption of current and new information security technologies implemented throughout the Agency.

i. Maintain a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA's Cybersecurity and Privacy Program.

j. Manage the NASA system of Record for all Assessment and Authorization artifacts, including all System Security Plans. The current System of Record is Risk Information Security Compliance System (RISCS).

k. Develop, implement and manage a High Value Asset (HVA) program in accordance with Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-02 Securing High Value Assets.

l. Develop, implement and manage a threat monitoring and incident response program, to include the NASA Security Operations Center, for NASA HVAs in accordance with DHS BOD 18-02.

m. Be an employee of the United States Federal Government.

1.2.3.5 A Center CISO shall:

a. Execute the Cybersecurity and Privacy Program at the Center level.

b. Assist the SAISO in enforcing NASA information security policies and procedures, and the Federal information security laws, directives, policies, and standards at the Center level.

1.2.3.6 An OCSO (if assigned per section 1.2.3.3) shall:

a. Ensure 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. Be an employee of the United States Federal Government.

1.2.3.7 The Center Cybersecurity Risk Manager (CCRM) shall:

a. Support the NASA cybersecurity Risk Executive function, as defined by NIST SP 800-37.

b. Serve as a cybersecurity risk management resource and as a subject matter expert on assessment and authorization for all personnel at their Center.

c. Provide oversight for the cybersecurity risk management activities carried out by Center and mission organizations to help ensure consistent and effective risk-based decisions, in accordance with NASA policies, procedures and organizational risk tolerance.

1.2.3.8 An AO shall:

a. Formally assume the responsibility for the operation of an information system or for the use of a designated set of common controls at an acceptable level of risk to the system, mission, and/or Agency.

b. Allocate sufficient resources to adequately protect information and information systems based on an assessment of organizational risks.

c. Assign Authorizing Official Designated Representatives (AODRs), as necessary. Once designated, an AO may not further delegate their risk acceptance role as AO. However, AOs are encouraged to assign AODRs to support AO visibility into, and management of, their information systems' cybersecurity posture.

d. Be an employee of the United States Federal Government.

1.2.3.9 An 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 An 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 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.

d. Allocate resources to protect information and information systems based on an assessment of system risks.

e. Ensure that information security controls are implemented according to a thorough risk-based analysis of their information systems' security postures.

f. Provide necessary assessment documentation, as required.

g. Take proper actions to identify, and minimize or eliminate, information system security deficiencies and weaknesses.

h. Communicate feedback to the Center CISO, OCSO (if assigned per section 1.2.3.3), 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 information system infrastructure.

k. Ensure that custom software developed for use on NASA information systems is implemented securely, in a manner that that reflects the criticality of its function, and the sensitivity of the information it generates, collects, processes, stores, or disseminates.

l. For a given program or project, develop a clear description of the information and system that is protected and evaluate the scope of information security resources that may be required for the project.

m. Appoint an Information Systems Security Officer (ISSO) to carry out provisions listed in 1.2.3.13.

1.2.3.11 Program Managers and Project Managers shall:

a. Allocate resources to protect information and information systems under their control based on an assessment of system risks.

b. Ensure identified cybersecurity risks accepted by AOs are also reflected in the program or project risk database(s)/system(s).

c. Include cybersecurity as part of the program and project plans for projects (e.g., incorporate the requirements of all applicable cybersecurity standards and specifications).

d. Identify and coordinate with ISOs for information systems under their control ensuring greater integration of cybersecurity and mission personnel.

e. Identify and coordinate with ISOs for information systems outside their control that support and impact their mission.

f. Ensure that all information systems under Program Managers' and Project Managers' control are fully compliant with the requirements of this directive.

1.2.3.12 An Information Owner (IO) shall:

a. Exercise statutory or operational authority for specified information.

b. Ensure the selection of information security controls is adequate for the protection of information under their authority during generation, collection, processing, dissemination, and disposal.

1.2.3.13 An Information System Security Officer (ISSO) shall:

a. Serve as the principal advisor to the ISO on issues regarding information security.

b. Ensure a proper operational security posture is maintained for their information system.

c. Be responsible for the day-to-day security operations of their information system.

1.2.3.14 Contracting Officers, as defined in Federal Acquisition Regulation 2.101, or Agreement Managers as defined in NAII 1050.3, NASA Partnership Guide, shall ensure that the requirements of this directive are included and in scope for all NASA contracts, Space Act agreements, cooperative agreements, partnership agreements, or other agreements pursuant to which NASA data is being processed and transmitted; IT devices are procured for a purpose that is not incidental to the contract, and/or IT devices are developed or used on a NASA network.

Chapter 2. Identify Function

2.1 Asset Management

2.1.1 Overview

2.1.1.1 Section 2.1 establishes requirements and processes to identify and manage data, devices, systems, and facilities relative to NASA's information security objectives and risk profile and risk posture.

2.1.2 Asset Management

2.1.2.1 The NASA SAISO shall ensure the maintenance of a NASA-wide information system inventory in the NASA system of record (i.e., RISCS).

2.1.2.2 An ISO shall:

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

b. Maintain, in the NASA system of record (i.e., RISCS), an accurate, up-to-date inventory of data, devices, systems, and facilities under their ownership monthly.

c. Provide such inventory to the Office of the Chief Information Officer (OCIO) in such manner and format that the SAISO determines.

2.1.3 Physical and Virtual Device and System Inventory

2.1.3.1 The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all physical and virtual devices and systems.

2.1.3.2 An ISO shall:

a. Ensure the inventory required by section 2.1.2.1 includes all physical and virtual devices and systems.

b. Provide the NASA SAISO with such inventory.

2.1.4 Software Platform and Application Inventory

2.1.4.1 The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all software platforms and applications.

2.1.4.2 The ISO shall:

a. Ensure the inventory required by section 2.1.2.1 includes all software platforms and applications.

b. Provide the NASA SAISO with such inventory.

2.1.5 System Interconnections

2.1.5.1 The NASA SAISO shall maintain the mapping of information system communications and data flows in the NASA system of record.

2.1.5.2 The ISO shall:

a. Maintain and update documentation regarding system interconnections.

b. Provide the NASA SAISO with a mapping of information system communications and data flows.

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

d. Review and update such MOAs, MOUs, and ISAs annually.

2.1.6 External Information Systems Catalog

2.1.6.1 The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all external information systems.

2.1.6.2 An ISO shall provide the NASA SAISO, in the NASA system of record (i.e., RISCS), with an inventory of external information systems under their supervision.

2.1.7 Resource Prioritization Policy

2.1.7.1 The SAISO shall consider the value of information and information systems to NASA's mission in the prioritization of information security effort and resources.

2.1.8 Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established in this section.

2.1.8.1 The NASA CIO shall:

a. Develop and maintain a NASA-wide Cybersecurity and Privacy Program.

b. Designate a SAISO.

2.1.8.2 The SAISO shall:

a. Manage the NASA Cybersecurity and Privacy Program.

b. Maintain and update, as needed to comply with federal and NASA requirements, NPD 2810.1, NPR 2810.1, and all related handbooks.

c. Publish and maintain such policies, procedures, NASA Information Technology Requirements (NITRs), specifications, standards, handbooks, and memoranda as may be necessary to implement the requirements of this directive.

2.2 Business Environment

2.2.1 Overview

2.2.1.1 This section establishes requirements to inform NASA's information security roles, responsibilities, and risk management decisions.

2.2.2 Supply Chain and Critical Infrastructure Identification

2.2.2.1 The NASA CIO shall:

a. Work with internal and external stakeholders to identify and communicate NASA’s role in the supply chain in order to inform the Supply Chain Risk Management (SCRM) requirements of section 2.6 of this document.

b. Work with internal and external stakeholders to identify and communicate NASA’s role in critical infrastructure.

2.2.3 Contingency Planning

2.2.3.1 The head of Center Protective Services and the Center CIO shall coordinate Center-wide contingency planning efforts that 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.

2.2.3.2 The SAISO shall:

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

b. Develop and test 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.

2.2.3.3 The Center CISO, in coordination with OPS, shall:

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

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

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

2.2.3.4 The ISO shall:

a. Develop, test, implement, and maintain information system contingency plans.

b. Document assessment, recovery, and restoration procedures.

c. Ensure 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 sufficient to permit a coordinated response at the Center and/or the Agency level.

f. Test, evaluate, and document contingency plans for accuracy, completeness, and effectiveness via a periodic test, training, and exercise program at a frequency in accordance with Agency Defined Values.

2.3 Governance

2.3.1 Overview

2.3.1.1 This section establishes the requirements to develop policies, procedures, and processes to manage and monitor NASA's regulatory, legal, and risk environment and operations relating to information security.

2.3.1.2 The tenets and framework of NASA's Cybersecurity and Privacy Program are spelled out in this directive and related handbooks, and the Cybersecurity and Privacy Program Plan. The policies, procedures, milestones, metrics, and responsibilities of the Cybersecurity and Privacy Program together make up the Cybersecurity and Privacy Program Plan.

2.3.2 Cybersecurity Policy

2.3.2.1 The SAISO shall:

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

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

c. Review, update, and augment the NASA Cybersecurity and Privacy Program.

d. Ensure that the NASA Cybersecurity and Privacy Program plan, policy, and requirements are implemented.

e. Update and disseminate Organization Defined Values via a cybersecurity specification updated at least annually.

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

g. With respect to unclassified information systems, be responsible for ensuring NASA's implementation of the NIST RMF.

2.3.2.2 The ISO shall maintain information security documentation in the NASA-wide information security document repository required by section 2.3.2.1b.

2.3.3 Coordination of Information Security

2.3.3.1 The SAISO shall:

2.3.3.2 Coordinate information security compliance with internal and external resources across the Agency.

a. 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).

b. Work with the NASA Office of Procurement to oversee the development and maintenance of an information security clause and coordinate implementation with NASA Office of Procurement as provided in the NASA Federal Acquisition Regulations (FAR), 48 CFR Ch. 18.

2.3.3.3 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.

2.3.3.4 Program Managers and Project Managers shall:

a. Ensure that projects or programs under their control implement the requirements of this directive.

b. Ensure that information security is incorporated into the planning and development of all information systems under their control by following the procedures outlined in NIST SP 800-160, Systems Security Engineering: Consideration for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems.

2.3.4 Management of legal and regulatory requirements

2.3.4.1 The SAISO shall:

a. Comply with OMB and FISMA reporting requirements.

b. Fulfill OMB and FISMA contingency plan testing requirements.

2.3.5 Governance and Management Processes

2.3.5.1 The NASA CIO shall report to OMB on the status of NASA's Cybersecurity and Privacy Program.

2.3.5.2 The SAISO shall:

a. Report to the NASA Administrator on the effectiveness of NASA's Cybersecurity and Privacy Program, including the progress of remedial actions, as required by FISMA.

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

2.3.5.3 The ISO shall:

a. Develop and maintain a System Security Plan (SSP) for their information systems.

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

c. Ensure that required system and services acquisition policy and procedures are implemented for their information systems and documented in the associated SSPs.

d. Establish system-level rules of behavior.

e. Assist in the development of information security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information.

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

2.4 Risk Assessment

2.4.1 Overview

2.4.1.1 This section establishes requirements for the assessment of cybersecurity risk to NASA's operations, assets, and individuals.

2.4.2 Risk Assessment Policy

2.4.2.1 The SAISO shall:

a. Identify and manage common cybersecurity threats to NASA.

b. Consistent with NPR 8000.4, Agency Risk Management Procedural Requirements, define and make available an RMF that describes a uniform methodology for risk assessment for all Agency internal and external systems.

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

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

e. Manage the NASA-wide information security performance metrics program.

f. Work with the Information Sharing and Analysis Centers (ISACs) and other relevant information sharing fora.

2.4.2.2 The Center CISO shall:

a. Identify and manage common threats to their Center.

b. Understand and communicate, with the AO, the ISO, the OCSO (if assigned), other Centers' CISOs, and the SAISO any cybersecurity flaws associated with any information system.

c. Verify the correct application of information system categorization criteria and requirements.

2.4.2.3 The OCSO (if assigned per section 1.2.3.3) shall:

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

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

2.4.2.4 The AO shall:

a. Authorize to operate only systems posing an acceptable level of risk to Agency assets, data, and personnel for production operation.

b. Ensure that all systems undergo a complete system security assessment prior to granting an initial Authorization to Operate (ATO).

c. Approve or reject information system categorizations.

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

e. Plan and assign resources for information security assessment and authorization activities.

2.4.2.5 The ISO shall:

a. Assess information systems for risk in accordance with Agency policy and procedures.

b. Create POA&Ms or provide a documented AO acceptance of risk related to any identified system information security deficiencies or weaknesses.

c. Complete POA&M tasks.

d. Apply resources towards the mitigation of identified risks to minimize threats to system performance.

e. 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.

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

g. Plan and advocate for the availability of resources for assessment and authorization activities.

h. Perform an information system risk analysis for their systems that can be used to support development of Agency information security baselines.

i. Seek an authorization from the AO prior to the operation of an information system and if changes to the system or its operating environment warrant a reauthorization.

2.4.2.6 The ISSO shall:

a. Perform information system risk analyses in support of security control selection and tailoring, security control implementation including system configuration, and continuous monitoring.

b. In collaboration with the ISO and IO(s), perform the information system security categorization, ensuring that the selected data types reflect all information generated, collected, processed and disseminated by the information system.

2.4.2.7 Program Managers and Project Managers shall:

a. With the support ISOs and ISSOs, understand and communicate to AOs any cybersecurity risks associated with any information system in a program or project under their control so that an assessment can be made of cybersecurity risk to Agency operations and resources.

b. Verify the proper application of information system categorization criteria and requirements for the programs and projects under their control.

2.5 Risk Management Strategy

2.5.1 Overview

2.5.1.1 This section establishes requirements for a cybersecurity risk management strategy to work in conjunction with requirements of NPR 8000.4.

2.5.2 Risk Management Strategy

2.5.2.1 The SAISO shall develop and implement a Cybersecurity Risk Management Strategy, which includes:

a. Definition of NASA's risk management priorities and constraints for NASA high-value assets, and mission and institutional systems.

b. Documentation criteria as a basis for determination of NASA's risk tolerances and assumptions.

c. Description of the importance of accurate and timely assessment of the likelihood and consequence severity of threats to NASA's critical infrastructure within the unique threat environment for NASA operations.

d. Ensure the underlying basis for risk acceptance decisions by AOs across NASA conform to validated practices set forth in NPR 8000.4.

2.6 Supply Chain Risk Management

2.6.1 Overview

2.6.1.1 This section establishes requirements for SCRM.

2.6.2 SCRM Policy

2.6.2.1 The NASA SAISO shall:

a. In awareness of Office of Safety and Mission Assurance roles, develop, manage, and update NASA's Cyber SCRM process.

b. Identify, prioritize, and assess suppliers and third-party partners of information systems using a cyber supply chain risk assessment process.

c. Work with program and procurement officials in NASA to ensure that:

(1) Contracts with suppliers and third-party partners implement measures designed to meet the objectives of this directive and the Cyber SCRM process required by section 2.6.2.1a.

(2) Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

(3) Response and recovery planning and testing are conducted with suppliers and third-party providers.

2.6.2.2 The ISO shall:

a. Understand the level of risk to an information system related to the information that is necessarily disclosed to vendors and suppliers during the acquisition process.

b. Establish a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

Chapter 3. Protect Function

3.1 Identity Management and Access Control

3.1.1 Overview

3.1.1.1 This section establishes requirements for identity management and access control.

3.1.1.2 NPR 2841.1, Identity, Credential, and Access Management (ICAM) establishes requirements for issuance, management, verification, and revocation of identities and credentials. Such identities and credentials govern both physical and logical access to NASA assets.

3.1.2 Physical Access Policy

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

3.1.2.2 The ISO shall:

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

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

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

3.1.2.3 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.

3.1.3 Remote Access Policy

3.1.3.1 The ISO shall:

a. Ensure only devices that are authorized and approved for remote access to the information system to which they are connecting are granted remote access in a manner consistent with organizational defined values.

b. Ensure that all remote access is routed through NASA CIO-authorized remote access points.

3.1.3.2 Program Managers and Project Managers shall ensure, with respect to any information system in a program or project under their control, that all remote access is routed through authorized NASA access control points.

3.1.3.3 The NASA User shall:

a. Use only NASA authorized and approved devices for remote access to NASA non-public information systems.

b. Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely and understand the consequences for mishandling.

3.1.4 Access Permissions and Authorization Policy

3.1.4.1 The ISO shall:

a. Administer accounts for their information systems in a way that provides separation of duties, avoids potential conflicts of interest, and grants NASA users the least privilege necessary to perform their respective duties.

b. Manage, in consideration of the IO, access to the information system, and with which privileges users will be authorized.

c. Ensure that any public facing service that requires a login is secured by multi-factor authentication (MFA).

d. Configure all systems and services to permit only authorized connections.

e. Manage all systems and services in a “deny by default, permit by exception” configuration for all ports, protocols, and services.

3.1.4.2 The IO may offer guidance to the ISO regarding management of access to the information system, and with which privileges users will be empowered.

3.1.4.3 The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the distribution and management of physical authenticators (i.e., PIV cards).

3.1.4.4 The NASA CIO shall ensure the distribution and management of any other authentication tokens.

3.1.5 Network Integrity Policy

3.1.5.1 The SAISO shall ensure that NASA maintains a Network Access Control Policy to monitor, control, prevent, or regulate device and system access to NASA networks.

3.1.6 Identity Policy

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

3.1.6.2 The ISO shall leverage the Agency identification and authentication framework for applications.

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

3.1.7 Authentication Policy

3.1.7.1 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 consent banner.

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

3.1.7.2 The ISO shall:

a. Leverage the Agency identification and authentication framework for applications.

b. Maintain account management capabilities (e.g., account creation, privilege configuration, maintenance, and deletion) for information systems.

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

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

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

3.2 Awareness and Training

3.2.1 Overview

3.2.1.1 This section establishes requirements for information security awareness and training to ensure that NASA's personnel and partners are trained to perform their cybersecurity-related duties and responsibilities consistent with NASA policies, procedures, and agreements.

3.2.2 Awareness and Training Policy

3.2.2.1 All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

3.2.2.2 The SAISO shall:

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

b. Define and make available all Agency information 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, and others.

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

d. Oversee the fulfillment of training requirements across the Agency and for external stakeholders, to include tracking and reporting on the completion of information security awareness and training requirements in the Agency system of record.

e. Maintain the NASA User Rules of Behavior and track user annual acceptance.

3.2.2.3 The ISO shall:

a. Allow access to information systems only to users who comply with all Agency information security awareness and training requirements.

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

3.2.2.4 The NASA User shall:

a. Comply with role-based information security and awareness training requirements.

b. Acknowledge acceptance of the Agency User Rules of Behavior annually.

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

3.3 Data Security

3.3.1 Overview

3.3.1.1 This section establishes requirements for data security to ensure that information and records are managed consistent with NASA's risk management policies and procedures to protect the confidentiality, integrity, and availability of information.

3.3.2 Data-at-Rest Protection Policy

3.3.2.1 The ISO shall ensure that information stored on, transmitted or processed by their information system is protected by encryption performed in accordance with a NIST approved encryption algorithm provided through either:

a. A FIPS-140-2 or FIPS-140-3 cryptographic module validated through the Cryptographic Module Validation Program (CMVP), or

b. A cryptographic module approved for the protection of classified national security information.

In the event that the use of encryption is technically unfeasible or would demonstrably affect the system's ability to carry out its respective mission, functions, or operations approval shall be granted in writing from the NASA CIO before an Authorizing Official may consider granting an Authorization to Operate.

3.3.2.2 The NASA User shall secure and protect media under their control using access restriction and/or sanitization (in accordance with the requirements of section 3.4.7.1).

3.3.3 Data-in-Transit Protection Policy

3.3.3.1 The ISO shall ensure that NASA information under their control is protected by suitable encryption when in transit.

3.3.4 Asset Management Policy

3.3.4.1 NPR 4200.1, NASA Equipment Management Procedural Requirements governs management of assets throughout removal, transfers, and disposition.

3.3.5 Protections Against Data Leakage

3.3.5.1 The NASA CIO shall ensure that NASA develops, implements, and maintains adequate data leakage protection for Agency common system and communications infrastructure.

3.3.5.2 The SAISO shall ensure the provision of Center-level boundary protection for systems that share a common infrastructure or services.

3.3.5.3 The Center CIO shall ensure the integration of software and hardware necessary to support system and communications requirements at their Center.

3.3.5.4 The ISO shall ensure shared resource policies, denial of service protections, boundary protection, and transmission integrity and confidentiality are implemented.

3.3.6 Development and Testing Environment Policy

3.3.6.1 The ISO shall ensure, to the extent practicable, the separation of development and testing environment(s) from production environment(s).

3.3.7 System and Information Integrity Policy

3.3.7.1 The SAISO shall:

a. Ensure that the capabilities 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).

b. Ensure that data is protected against unauthorized access, tampering, alteration, loss, and destruction.

3.3.7.2 The ISO shall:

a. Implement data integrity protections on their information systems.

b. Test information system security functions in accordance with requirements, and document the frequency and processes related to the tests.

3.4 Information Protection Processes and Procedures

3.4.1 Overview

3.4.1.1 This section establishes securities, processes, and procedures to manage protection of information systems and assets.

3.4.2 Information Security Baseline Configuration Policy

3.4.2.1 The SAISO shall:

a. Create and maintain processes for development, approval, distribution, and verification of information security configuration baselines for covered articles, incorporating, for example, the concept of least functionality.

b. Create and maintain processes to monitor information security baseline configuration compliance.

c. Ensure information security baseline configurations conform to federal guidelines and requirements.

3.4.2.2 The ISO shall implement the requirements and settings defined in all applicable standards and specifications established by the Agency Security Configuration Standards (ASCS).

3.4.3 System Development Life Cycle Policy

3.4.3.1 The ISO shall ensure information security considerations are managed throughout their systems' development life cycle to protect NASA information.

3.4.4 Configuration Change Control Policy

3.4.4.1 The ISO shall create, implement, and maintain configuration change control policies and processes for their system as needed.

3.4.5 Backups of information

3.4.5.1 ISOs shall back up user-level and system-level information.

3.4.6 Physical Operating Environment Policy

3.4.6.1 The SAISO shall coordinate with OPS to ensure the development and maintenance standards and guidance for security of NASA information systems’ physical operating environments.

3.4.7 Data Destruction Policy

3.4.7.1 NASA policy is to facilitate suitable media sanitization and destruction of no longer needed data to reduce the risk of leakage of non-public NASA information to unauthorized persons or entities; provided, however, that such destruction only occurs in accordance with laws, regulations, guidance, and other NASA policies or directives governing retention and other aspects of data management.

3.4.7.2 The Center CISO shall ensure, in coordination with the Center Security Office, that sufficient equipment or services are available to facilitate media sanitization and data destruction in accordance with policy.

3.4.7.3 The OCSO (if assigned per section 1.2.3.3) shall be responsible for the sanitization of media and destruction of data according to policy for their organization.

3.4.7.4 The ISO shall be responsible for the sanitization of media and destruction of data according to policy for their information system.

3.4.7.5 The NASA User shall mitigate the risks of leakage of non-public NASA information to unauthorized persons or entities through the sanitization of media and destruction of data according to policy.

3.4.8 Protection Processes Improvement Policy

3.4.8.1 The SAISO shall identify, implement, and maintain a NASA-wide resource for the management of corrective action plans to mitigate information system security weaknesses.

3.4.8.2 The OCSO (if assigned per section 1.2.3.3) shall review and update their organization's SSPs in accordance with this directive and its associated handbooks.

3.4.8.3 The ISO shall review and update SSPs in accordance with this directive and its associated handbooks.

3.4.9 Effectiveness of Protection Technology

The SAISO shall ensure that the effectiveness of protection technology (e.g. continuous monitoring tools) is measured and shared to improve NASA's information security posture.

3.4.10 Information Security and Human Resources Policy

3.4.10.1 The SAISO shall make all offices aware of requirements and expectations related to ICAM.

3.4.10.2 The Center CISO shall confirm that all personnel adhere to the limits of their delegated cybersecurity authority.

3.4.10.3 The ISO shall:

a. Provide oversight to ensure that personnel adhere to limits on access to information and information systems.

b. Manage or terminate access to secured resources following the transfer or termination of personnel.

3.4.10.4 The Center Chief of Security under the policy guidance of the Assistant Administrator of Office of Protective Services shall implement personnel security controls.

3.4.11 Vulnerability Management

3.4.11.1 The SAISO shall:

a. Develop and maintain a Vulnerability Management Plan.

b. Establish processes and systems for the management of vulnerability, flaw remediation, and information system monitoring.

c. Ensure the proper handling of vulnerability and 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.

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

3.4.11.3 The ISO shall:

a. Ensure the completion of vulnerability and flaw remediation activities, and document and communicate residual risks, as necessary in accordance with Federal and Agency requirements.

b. Ensure that software updates and patches remediating security flaws are applied to their system in accordance with Federal and Agency requirements.

3.5 Maintenance

3.5.1 Overview

3.5.1.1 This section establishes requirements related to maintenance and repair (including remote maintenance) of information systems.

3.5.2 Maintenance and Repair Policy

3.5.2.1 The ISO shall:

a. Develop, maintain, and implement 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.

d. Ensure that maintenance is logged for their system.

3.6 Protective Technology

3.6.1 Overview

3.6.1.1 This section establishes requirements for management of technical information security solutions to ensure the security and resilience of systems and assets.

3.6.2 Audit and Logging Records Policy

3.6.2.1 The NASA CIO shall ensure the development and maintenance of a capability for the aggregation of NASA-wide information system logs.

3.6.2.2 The SAISO shall:

a. Maintain Agency information system record retention policies for logs, and minimum auditable events.

b. Develop and maintain log information security auditing capabilities for NASA information system logs.

3.6.2.3 The ISO shall:

a. Maintain auditing capabilities for their information system components.

b. Allocate audit record storage capacity for an information system in accordance with Agency records retention requirements.

c. Determine the 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.

d. Ensure audit logs are 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 of the log.

e. Ensure data in information systems are retained or destroyed in accordance with NASA Records Retention Schedule No 1441.1 (updated) May 18, 2020. .

3.6.3 Media Protection Policy

3.6.3.1 The Center CISO shall:

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

b. Use encryption solutions that are compliant with federal encryption standards, NIST guidance, and are in accordance with NASA requirements regarding the protection of sensitive information to guard portable and removable digital media devices.

3.6.3.2 The NASA User shall:

a. Protect removable media devices.

b. Use only media that complies with NASA Media Use Policy (as detailed in ITS-HBK-2810.11-2B Media Protection and Sanitization, Appendix C.)

c. Mitigate the risks of data loss by securing and protecting media under their control and the information contained within those devices through encryption, access restriction, and sanitization.

3.6.3.3 The OCSO (if assigned per section 1.2.3.3), in collaboration with ISOs, shall protect and sanitize media for their organization, including the protection of data at rest.

3.6.3.4 The ISO shall protect and sanitize media for their information system, including the protection of data at rest.

Chapter 4. Detect Function

4.1 Anomalies and Events

4.1.1 Overview

4.1.1.1 This section establishes requirements and processes for detection of anomalous activity and understanding such activity's potential impact.

4.1.2 Anomaly and Event Detection Policy

4.1.2.1 The CIO shall collect information from the ISOs to determine the baseline of network operations and expected data flows for users and systems.

4.1.2.2 The SAISO shall:

a. Ensure the capability to detect anomalous events on NASA information systems and networks.

b. Establish procedures for detecting, analyzing, and responding to anomalous events.

4.1.2.3 The ISO shall provide the CIO with a baseline of network operations and expected data flows for systems under their control.

4.1.2.4 The ISSO shall assist in developing event containment and remediation strategies to minimize impact to an information system.

4.2 Security Continuous Monitoring

4.2.1 Overview

4.2.1.1 This section establishes requirements for continuous monitoring of information systems.

4.2.2 Continuous Monitoring Policy

4.2.2.1 The SAISO shall:

a. Develop and implement a strategy for continuous monitoring of NASA information systems.

b. Define the acceptability, and requirements for use, of cybersecurity monitoring tools for use across the agency.

4.2.2.2 The ISO shall:

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

b. Ensure that SAISO-required cybersecurity monitoring tools are deployed to all components of their information system to collect information, and to track all events of interest.

c. Develop and implement a strategy for continuous monitoring of their information system, which is consistent with the Agency strategy for continuous monitoring.

d. Perform continuous monitoring of their information system and keep the AO informed of continuous monitoring results in support of the ongoing authorization of their information system, in accordance with NASA's implementation of the RMF.

4.2.2.3 The Center CISO, supported by the CCRM, shall meet all continuous monitoring requirements.

4.2.3 Malicious and Unauthorized Code Detection Policy

4.2.3.1 The SAISO shall:

a. Define requirements for tools to detect malicious or unauthorized software and malicious or unauthorized changes to software or configuration.

b. Ensure such detection capability extends to mobile devices having access to NASA networks.

4.2.3.2 The ISO shall ensure their system uses SAISO-required tools to detect malicious or unauthorized software and malicious or unauthorized changes to software or configuration.

4.2.4 Vulnerability Scanning Policy

4.2.4.1 The SAISO shall:

a. Define requirements for tools to scan NASA information systems for vulnerabilities.

b. Regularly review and approve the use of Agency tools for vulnerability scanning.

4.2.4.2 The Center CIO shall ensure vulnerability scanning and remediation activities are being conducted at their Center using SAISO-required tools.

4.2.4.3 The Center CISO shall ensure that all information systems and devices on NASA networks are scanned for vulnerabilities.

4.2.4.4 The ISSO shall ensure that their information systems are regularly scanned for vulnerabilities or flaws that will then be remediated using SAISO-required tools, per 3.4.11.3.

4.3 Detection Processes

4.3.1 Overview

4.3.1.1 This section establishes requirements for detection processes and procedures.

4.3.2 Detection Process Policy

4.3.2.1 The SAISO shall:

a. Ensure that detection processes and procedures comply with all requirements (e.g., law, regulations, guidance, or other NASA NPDs and NPRs).

b. Establish a process to test and continuously improve detection processes and procedures.

Chapter 5. Respond Function

5.1 Response Planning

5.1.1 Overview

5.1.1.1 This section establishes requirements for processes and procedures to ensure response to an Incident.

5.1.1.2 An incident response and management capability is necessary for rapidly responding to 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.

5.1.2 Incident Response Planning Policy

5.1.2.1 The CIO shall allocate resources for a NASA-wide SOC and Incident Response Teams.

5.1.2.2 The SAISO shall:

a. Implement and manage a NASA-wide SOC.

b. Designate an Agency Incident Response Manager for cybersecurity incidents.

c. Develop and maintain a NASA-wide Incident Response Plan, which shall contain processes and procedures for detecting, reporting, analyzing, and responding to information security incidents.

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

5.1.2.3 The Center CIO shall support information security investigations.

5.1.2.4 The Center CISO shall:

a. Coordinate with the SOC and the Agency Incident Response Manager to assist all incident response efforts and management policies, procedures, investigations, and reporting for all information systems at their Center.

b. Support the SOC and the Agency Incident Response Manager with all incident response tests, training, and exercises for their Center information systems.

5.2 Communications

5.2.1 Overview

5.2.1.1 This section establishes requirements for the communications and coordination elements of a response to an incident.

5.2.2 Incident Communications and Coordination Policy

5.2.2.1 The SAISO shall:

a. Include elements providing for coordination with internal and external stakeholders (e.g., external support from law enforcement agencies) in the incident response plan required by section 5.1.2.2c.

b. Support investigations into information security incidents related to criminal activity, counterintelligence, or counterterrorism.

c. Support investigations into information security incidents initiated by the Office of the General Counsel, the Office of Chief Human Capital Officer, 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.

e. Ensure that incidents are reported to external agencies as directed by laws and regulations.

5.2.2.2 The Center CISO coordinates between the incident response team and the Center privacy managers regarding breach response and handling of incidents related to sensitive information.

5.2.2.3 The ISO shall:

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

b. Handle incident information in accordance with all data sensitivity requirements.

c. Support information security investigations.

5.2.2.4 The ISSO shall report all suspected or confirmed information security incidents in a timely manner.

5.2.2.5 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).

5.3 Analysis

5.3.1 Overview

5.3.1.1 This section establishes requirements for analysis to ensure effective response and support recovery activities.

5.3.2 Incident Analysis Policy

5.3.2.1 The SAISO shall include elements in the Incident Response Plan that provide for analysis of information security incidents as required by section 5.1.2.2c.

5.4 Mitigation

5.4.1 Overview

5.4.1.1 This section establishes requirements for activities to be performed to prevent expansion of an event, mitigate its effects, and resolve an event.

5.4.2 Incident Mitigation Policy

5.4.2.1 The SAISO shall include elements that provide for containment and mitigation of information security incidents in the Incident Response Plan required by section 5.1.2.2c.

5.5 Improvements

5.5.1 Overview

5.5.1.1 This section establishes requirements for improvement of response detection and activities.

5.5.2 Incident Response Improvement Policy

5.5.2.1 The SAISO shall incorporate lessons learned from current or prior information security incidents in the Incident Response Plan required by section 5.1.2.2c.

Chapter 6. Recover Function

6.1 Recovery Planning

6.1.1 Overview

6.1.1.1 This section establishes requirements for processes and procedures to ensure recovery from an incident.

6.1.2 Incident Recovery Planning Policy

6.1.2.1 The SAISO shall develop and maintain a NASA-wide Incident Recovery Plan, which contains processes and procedures for incorporating lessons learned from incident response activities. The Incident Recovery Plan may be executed during or after information security incidents and may be included in the Incident Response Plan

6.2 Improvements

6.2.1 Overview

6.2.1.1 This section establishes requirements for the improvement of incident recovery efforts.

6.2.2 Incident Recovery Improvement Policy

6.2.2.1 The SAISO shall incorporate lessons learned from current or prior incidents in the Incident Recovery Plan required by section 6.1.2.1.

6.3 Communications

6.3.1 Overview

6.3.1.1 This section establishes requirements for communications to internal and external stakeholders regarding recovery from an Incident.

6.3.2 Incident Recovery Communications and Coordination Policy

6.3.2.1 The SAISO shall ensure the plan required by section 6.1.2.1 includes:

a. A public relations management strategy that works to restore trust in NASA’s mission capabilities.

b. Procedures for communications with internal and external stakeholders as well as executive and management teams.

Appendix A Definitions

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.

Boundary Protection. The security safeguards or countermeasures in place on an information system's logical and physical perimeters.

Common Control. A security safeguard or countermeasure which may be designed, implemented, and assessed at a level which encompasses one or more information systems.

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.

Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyberspace. The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Data Security. The combination of data-at-rest protection and data-in-transit protection that provides the confidentiality, availability, and integrity of data.

Elevated Privileges. A set of capabilities allowing a user to perform security-relevant functions.

External Information System. Any information system owned, operated, and managed by outside agencies, contractors, universities, or other organizations which store, process, or disseminate NASA-owned data under a contract or formal agreement, such as an interagency agreement, with NASA.

External information systems may be owned by outside agencies, contractors, universities, or other organizations and provide services to other customers besides NASA. These systems are usually not located on NASA owned/lease facilities, usually do not use NASA internet protocol (IP) addresses, and usually do not use NASA domain name service (DNS) entries.

Handbook. An Agency-level, SAISO-approved document which prescribes the best practices, policies, and procedures regarding various information system security topics.

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.

Information. Any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, produced for, or is under the control of NASA.

Information Security. The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Baseline. Predefined sets of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest.

Information Security Incident. Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality. For example, 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.

Information System. A discrete set of resources designed and implemented for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This term includes both Operational Technology and Information Technology.

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Internal Information System. A system that is generally covered by an SSP developed by NASA or its contractors and exists for the sole purpose of supporting NASA's mission or operations. These systems are often located on/at NASA owned/leased facilities, use NASA IP addresses, and/or use NASA DNS entries. Also called a NASA system or an Agency system.

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.

Media. Physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system.

NASA Center. Any of the collection of facilities and installations designated by NASA, and usually grouped by function (e.g., research, construction, administration).

NASA User. Any explicitly authorized patron of a NASA information system.

Near Real-Time (Risk Assessment). An analysis of an information system's security posture which closely reflects the immediate state of the system.

Network. A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Ongoing Authorizations. The continuous acceptance of an information system's operation based on a real-time understanding of the system's security posture.

Operational Control. The collection of strategic NIST SP 800-53 controls dedicated to information system security.

Operational Technology. Operational Technology: Hardware and software that is physically part of, dedicated to, or essential in real time to the performance, monitoring, or control of physical devices and processes..

Organization Defined Values. Those details of certain security controls that are meant to be determined by the managing entity.

Typically, a memo delivered annually by the OCIO that defines specific details of a security control's implementation.

Physical Devices and Systems. A tangible asset that is used in the acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.

Privileged User. A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Program. A strategic investment by a Mission Directorate or Mission Support Office that has a defined architecture and/or technical approach, requirements, funding level, and a management structure that initiates and directs one or more projects. A program defines a strategic direction that the Agency has identified as needed to accomplish Agency goals and objectives.

Program Manager. A generic term for the person who is formally assigned to be in charge of the program. A program manager could be designated as a program lead, program director, or some other term, as defined in the program's governing document.

Project. A specific investment identified in a Program Plan having defined requirements, a life-cycle cost, a beginning, and an end. A project also has a management structure and may have interfaces to other projects, agencies, and international partners. A project yields new or revised products that directly address NASA's strategic needs.

Project Manager. A generic term that represents the position in charge of the project. A project manager could be designated as a project lead, project principal investigator, project scientist, research director, project executive, or some other term, as defined in the project's governing document.

Risk Assessment. The value-based analysis of an information system's security posture.

Risk Management. The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

Security Posture. The overall state of an information system's confidentiality, integrity, and availability in the face of an ever-changing risk landscape.

Security-relevant function. Any manner of process or range of capabilities that can potentially impact the operation or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

System Development Life Cycle. The full scope of activities conducted by ISOs associated with a system during its lifespan. The lifecycle begins with the project initiation phase and ends with the system disposal phase.

Technical Control. The collection of tactical NIST SP 800-53 controls dedicated to information system security.

Appendix B Acronyms

AO	Authorizing Official
AoA	Analysis of Alternatives
AODR	Authorizing Official Designated Representative
ASCS	Agency Security Configuration Standards
ATO	Authorization to Operate
BOD	Binding Operational Directive
C2	Command and Control
CCRM	Center Cyber Risk Manager
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSI	Classified National Security Information
COOP	Continuity of Operations Planning
CSF	Cyber Security Framework
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DNS	Domain Name System
E.O.	Executive Order
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FR	Federal Register
GAO	Government Accountability Office
GOCO	Government Owned, Contractor Operated
HBK	Handbook
HSPD	Homeland Security Presidential Directive
HVA	High-Value Asset

ICAM	Identity, Credential, and Access Management
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IO	Information Owner
IPTA	Information and Privacy Threshold Analysis
ISA	Interconnection Security Agreement
ISAC	Information Sharing and Analysis Center
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
JPL	Jet Propulsion Laboratory
MDR	Mission Definition Review
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NODIS	NASA Online Directives System
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NRRS	NASA Records Retention Schedules
NTISS	National Telecommunications and Information System Security
OCIO	Office of the Chief Information Officer
OCSO	Organizational Computer Security Official
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPS	Office of Protective Services
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
PM	Program/Project Manager
POA&M	Plan of Action & Milestones
PRR	Production Readiness Review
RISCS	Risk Information Security Compliance System
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAR	Security Control Assessment Report
SAP	Security Assessment Plan
SCA	Security Control Assessor
SCAR	Security Control Assessment Report
SCRM	Supply Chain Risk Management
SOC	Security Operations Center
SP	Special Publication
SRR	System Requirements Review
SSP	System Security Plan
TRR	Test Readiness Review
U.S.C.	United States Code

Appendix C Requirements Matrices

C.1 AO

Para #	Requirement
1.2.3.8a	Formally assume the responsibility for the operation of an information system or for the use of a designated set of common controls at an acceptable level of risk to the system, mission, and/or Agency.
1.2.3.8b	Allocate sufficient resources to adequately protect information and information systems based on an assessment of organizational risks.
1.2.3.8c	Assign Authorizing Official Designated Representatives (AODRs), as necessary.
1.2.3.8d	Be an employee of the United States Federal Government.
2.4.2.4a	Authorize to operate only systems posing an acceptable level of risk to Agency assets, data, and personnel for production operation.
2.4.2.4b	Ensure that all systems undergo a complete system security assessment prior to granting an initial Authorization to Operate (ATO).
2.4.2.4c	Approve or reject information system categorizations.
2.4.2.4d	Grant or deny systems ATO based on an evaluation of risk to the security posture of their information systems.
2.4.2.4e	Plan and assign resources for information security assessment and authorization activities.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.2 AODR

Para #	Requirement
1.2.3.9a	Execute the responsibilities of the AO as delegated.
1.2.3.9b	Be an employee of the United States Federal Government.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.3 Assistant Administrator of Procurement

Para #	Requirement
2.3.3.3a	Ensure that contracting officials are aware of requirements related to information security.
2.3.3.3b	Ensure the inclusion of information security requirements in all contracts and solicitations.

C.4 Assistant Administrator of the Office of Protective Services

Para #	Requirement
3.1.4.3	The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the distribution and management of physical authenticators (i.e., PIV cards).

C.5 Assistant Administrator of the Office of the Chief Human Capital Officer

Para #	Requirement
3.2.2.5	The Assistant Administrator of the Office of the Chief Human Capital Officer shall ensure the availability of a NASA-wide platform for training delivery, as well as training results and training records management.

C.6 Center Chief of Security

Para #	Requirement
3.1.2.3a	Ensure the implementation of physical and environmental security controls.
3.1.2.3b	Ensure the capability to monitor physical and environmental security controls.
3.1.4.3	The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the distribution and management of physical authenticators (i.e., PIV cards).
3.4.10.4	The Center Chief of Security under the policy guidance of the Assistant Administrator of Office of Protective Services shall implement personnel security controls.

C.7 Center CIO

Para #	Requirement
1.2.3.2a	Execute the responsibilities, comparable to those of the NASA CIO, at the Center level.
1.2.3.2b	Execute the responsibilities, comparable to those of the NASA CIO, with respect to NASA facilities and systems not located at a Center as designated by the CIO.
1.2.3.2c	If the Center CIO assigns an Organizational Computer Security Official (OCSO) per section 1.2.3.3, designate Center-specific OCSO responsibilities, and any necessary interfaces with the Center CISO, in a Center-level formal policy.
1.2.3.2d	Be an employee of the United States Federal Government.
1.2.3.3	A Center CIO may optionally assign OCSOs to facilitate the implementation and oversight of information security within their organization.
2.2.3.1	The head of Center Protective Services and the Center CIO shall coordinate Center-wide contingency planning efforts that 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.
3.1.2.1	The Center CIO shall work with the Center Chief of Security, and the Center Facilities organization to ensure physical and environmental controls are met for the information systems at their Centers.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.3.5.3	The Center CIO shall ensure the integration of software and hardware necessary to support system and communications requirements at their Center.
4.2.4.2	The Center CIO shall ensure vulnerability scanning and remediation activities are being conducted at their Center using SAISO-required tools.
5.1.2.3	The Center CIO shall support information security investigations.

C.8 Center CISO

Para #	Requirement
1.2.3.5a	Execute the Cybersecurity and Privacy Program at the Center level.
1.2.3.5b	Assist the SAISO in enforcing NASA information security policies and procedures, and the Federal information security laws, directives, policies, and standards at the Center level.
2.2.3.3a	Ensure implementation of those information system contingency planning procedures that provide for notification, activation, response, recovery, and reconstitution.
2.2.3.3b	Oversee and arbitrate conflict resolution for all Center-wide information system contingency plans.
2.2.3.3c	Ensure and support information system contingency plan tests, training, and exercises.
2.4.2.2a	Identify and manage common threats to their Center.
2.4.2.2b	Understand and communicate, with the AO, the ISO, the OCSO (if assigned), other Centers' CISOs, and the SAISO any cybersecurity flaws associated with any information system.
2.4.2.2c	Verify the correct application of information system categorization criteria and requirements.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.4.7.2	The Center CISO shall ensure, in coordination with the Center Security Office, that sufficient equipment or services are available to facilitate media sanitization and data destruction in accordance with policy.
3.4.10.2	The Center CISO shall confirm that all personnel adhere to the limits of their delegated cybersecurity authority.
3.4.11.2	The Center CISO shall facilitate the implementation of NASA flaw remediation policies and procedures at their Center.
3.6.3.1a	Ensure, in coordination with the Center Security Office, that sufficient equipment and services are available to facilitate media sanitization.
3.6.3.1b	Use encryption solutions that are compliant with federal encryption standards, NIST guidance, and are in accordance with NASA requirements regarding the protection of sensitive information to guard portable and removable digital media devices.
4.2.2.3	The Center CISO, supported by the CCRM, shall meet all continuous monitoring requirements.
4.2.4.3	The Center CISO shall ensure that all information systems and devices on NASA networks are scanned for vulnerabilities.
5.1.2.4a	Coordinate with the SOC and the Agency Incident Response Manager to assist all incident response efforts and management policies, procedures, investigations, and reporting for all information systems at their Center.
5.1.2.4b	Support the SOC and the Agency Incident Response Manager with all incident response tests, training, and exercises for their Center information systems.
5.2.2.2	The Center CISO shall coordinate between the incident response team and the Center privacy managers regarding breach response and handling of incidents related to sensitive information.

C.9 Center Cybersecurity Risk Manager

Para #	Requirement

1.2.3.7a	Support the NASA cybersecurity Risk Executive function, as defined by NIST SP 800-37.
1.2.3.7b	Serve as a cybersecurity risk management resource and as a subject matter expert on assessment and authorization for all personnel at their Center.
1.2.3.7c	Provide oversight for the cybersecurity risk management activities carried out by Center and mission organizations to help ensure consistent and effective risk-based decisions, in accordance with NASA policies, procedures and organizational risk tolerance.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.10 Center Directors and the Director for Headquarters Operations

Para #	Requirement
1.2.2.5a.	With concurrence from the SAISO and the Center's CIO, designate a Center Chief Information Security Officer (CISO) in writing.
1.2.2.5b.	Ensure the Center CISO has adequate staff, resources, budget, and authority to implement information security programs at their Center.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.11 CIO

Para #	Requirement
1.2.2.3a	Ensure confidentiality, integrity, and availability of all NASA's information assets throughout the system life cycle.
1.2.2.3b	Ensure all NASA IT is in compliance with federal and NASA Cybersecurity and Privacy Program requirements.
1.2.2.3c	Commission suitable governance bodies.
1.2.2.3d	Evaluate and approve the designation of Authorizing Officials (AO).
1.2.2.3e	Advise senior NASA officials concerning their information security responsibilities.
1.2.2.3f	Ensure the NASA enterprise architecture integrates information security considerations into the strategic, capital, and investment planning process.
1.2.2.3g	Encourage the maximum reuse and sharing of information security-related information throughout the NASA community.
1.2.2.3h	Develop, implement, and maintain a Controlled Unclassified Information (CUI) program which is managed in accordance with Executive Order (E.O.) 13556, Controlled Unclassified Information, and 32 CFR Part 2002, Controlled Unclassified Information.
1.2.2.3i	Be an employee of the United States Federal Government.
2.1.8.1a	Develop and maintain a NASA-wide Cybersecurity and Privacy Program.
2.1.8.1b	Designate a SAISO.
2.2.2.1a	Work with internal and external stakeholders to identify and communicate NASA's role in the supply chain in order to inform the Supply Chain Risk Management (SCRM) requirements of section 2.6 of this document.
2.2.2.1b	Work with internal and external stakeholders to identify and communicate NASA's role in critical infrastructure.

2.3.5.1	Report to OMB on the status of NASA's Cybersecurity and Privacy Program.
3.1.4.4	The NASA CIO shall ensure the distribution and management of any other authentication tokens.
3.1.6.1	The NASA CIO shall provide a NASA-wide framework for identity and authentication management.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.3.5.1	The NASA CIO shall ensure that NASA develops, implements, and maintains adequate data leakage protection for Agency common system and communications infrastructure.
3.6.2.1	The NASA CIO shall ensure the development and maintenance of a capability for the aggregation of NASA-wide information system logs.
4.1.2.1	The CIO shall collect information from the ISOs to determine the baseline of network operations and expected data flows for users and systems.
5.1.2.1	The CIO shall allocate resources for a NASA-wide SOC and Incident Response Teams.

C.12 Contracting Officers or Agreement Managers

Para #	Requirement
1.2.3.14	Contracting Officers, as defined in Federal Acquisition Regulation 2.101, or Agreement Managers as defined in NASA Advisory Implementing Instruction 1050.3B shall ensure that the requirements of this directive are included and in scope for all NASA contracts, Space Act agreements, cooperative agreements, partnership agreements, or other agreements pursuant to which NASA data is being processed and transmitted; IT devices are procured for a purpose that is not incidental to the contract, and/or IT devices are developed or used on a NASA network.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.13 Head of Center Protective Services

Para #	Requirement
2.2.3.1	The head of Center Protective Services and the Center CIO shall coordinate Center-wide contingency planning efforts that 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.

C.14 IO

Para #	Requirement
1.2.3.12a	Exercise statutory or operational authority for specified information.
1.2.3.12b	Ensure the selection of information security controls is suitable for the protection of information under their authority during generation, collection, processing, dissemination, and disposal.
3.1.4.2	The IO may offer guidance to the ISO regarding management of access to the information system, and with which privileges users will be empowered.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.15 ISO

Para #	Requirement
1.2.3.10a	Acquire, develop, integrate, operate, modify, maintain, and dispose of information systems.
1.2.3.10b	Ensure system-level implementation of all Agency and Center requirements.
1.2.3.10c	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.
1.2.3.10d	Allocate resources to protect information and information systems based on an assessment of system risks.
1.2.3.10e	Ensure that information security controls are implemented according to a thorough risk-based analysis of their information systems' security postures.
1.2.3.10f	Provide necessary assessment documentation, as required.
1.2.3.10g	Take proper actions to identify, and minimize or eliminate, information system security deficiencies and weaknesses.
1.2.3.10h	Communicate feedback to the Center CISO, OCSO (if assigned per section 1.2.3.3), and AO regarding the impact of Agency and Center-wide information security requirements on the operation of their information systems.
1.2.3.10i	Ensure funding requests for information security requirements are included in annual budgeting submissions.
1.2.3.10j	Utilize, to the extent possible, Agency-provided information system infrastructure.
1.2.3.10k	Ensure that custom software developed for use on NASA information systems is implemented securely, in a manner that that reflects the criticality of its function, and the sensitivity of the information it generates, collects, processes, stores, or disseminates.
1.2.3.10l	For a given program or project, develop a clear description of the information and system that is protected and evaluate the scope of information security resources that may be required for the project.
1.2.3.10m	Appoint an Information Systems Security Officer (ISSO) to carry out provisions listed in 1.2.3.13.
2.1.2.2a	Ensure that information system components are identified and documented.
2.1.2.2b	Maintain, in the NASA system of record (i.e., RISCS), an accurate, up-to-date inventory of data, devices, systems, and facilities under their ownership monthly.
2.1.2.2c	Provide such inventory to the Office of the Chief Information Officer (OCIO) in such manner and format that the SAISO determines.
2.1.3.2a	Ensure the inventory required by section 2.1.2.1 includes all physical and virtual devices and systems.
2.1.3.2b	Provide the NASA SAISO with such inventory.
2.1.4.2a	Ensure the inventory required by section 2.1.2.1 includes all software platforms and applications.
2.1.4.2b	Provide the NASA SAISO with such inventory.
2.1.5.2a	Maintain and update documentation regarding system interconnections.

2.1.5.2b	Provide the NASA SAISO with a mapping of information system communications and data flows.
2.1.5.2c	Develop Memoranda of Agreements (MOA), Memoranda of Understandings (MOU), and Interconnection Security Agreements (ISA) for their systems.
2.1.5.2d	Review and update such MOAs, MOUs, and ISAs annually.
2.1.6.2	An ISO shall provide the NASA SAISO, in the NASA system of record (i.e., RISCS), with an inventory of external information systems under their supervision.
2.2.3.4a	Develop, test, implement, and maintain information system contingency plans.
2.2.3.4b	Document assessment, recovery, and restoration procedures.
2.2.3.4c	Ensure that the contingency plan documentation is maintained in a ready state and accurately reflects system requirements, procedures, organizational structure, and policies.
2.2.3.4d	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.
2.2.3.4e	Ensure that information system contingency plan documentation is at a level sufficient to permit a coordinated response at the Center and/or the Agency level.
2.2.3.4f	Test, evaluate, and document contingency plans for accuracy, completeness, and effectiveness via a periodic test, training, and exercise program at a frequency in accordance with Agency Defined Values.
2.3.2.2	Maintain information security documentation in the NASA-wide information security document repository required by section 2.3.2.1b.
2.3.5.3a	Develop and maintain a System Security Plan (SSP) for their information systems.
2.3.5.3b	Ensure that all SSPs are developed and tailored to address the threats and associated risks faced by the system.
2.3.5.3c	Ensure that required system and services acquisition policy and procedures are implemented for their information systems and documented in the associated SSPs.
2.3.5.3d	Establish system-level rules of behavior.
2.3.5.3e	Assist in the development of information security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information.
2.4.2.5a	Assess information systems for risk in accordance with Agency policy and procedures.
2.4.2.5b	Create POA&Ms or provide a documented AO acceptance of risk related to any identified system information security deficiencies or weaknesses.
2.4.2.5c	Complete POA&M tasks.
2.4.2.5d	Apply resources towards the mitigation of identified risks to minimize threats to system performance.
2.4.2.5e	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.
2.4.2.5f	Inform key officials of pending assessment and authorization activities.
2.4.2.5g	Plan and advocate for the availability of resources for assessment and authorization activities.
2.4.2.5h	Perform an information system risk analysis for their systems that can be used to support development of Agency information security baselines.

2.4.2.5i	Seek an authorization from the AO prior to the operation of an information system and if changes to the system or its operating environment warrant a reauthorization.
2.6.2.2a	Understand the level of risk to an information system related to the information that is necessarily disclosed to vendors and suppliers during the acquisition process.
2.6.2.2b	Establish a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.
3.1.2.2a	Approve personnel access to secured or restricted physical information system facilities and locations.
3.1.2.2b	Establish and maintain a list of all personnel authorized to access secured or restricted physical information system facilities and locations.
3.1.2.2c	Validate physical and environmental security controls and monitoring capabilities.
3.1.3.1a	Ensure only devices that are authorized and approved for remote access to the information system to which they are connecting are granted remote access in a manner consistent with organizational defined values.
3.1.3.1b	Ensure that all remote access is routed through NASA CIO-authorized remote access points.
3.1.4.1a	Administer accounts for their information systems in a way that provides separation of duties, avoids potential conflicts of interest, and grants NASA users the least privilege necessary to perform their respective duties.
3.1.4.1b	Manage, in consideration of the IO, access to the information system, and with which privileges users will be authorized.
3.1.4.1c	Ensure that any public facing service that requires a login is secured by multi-factor authentication (MFA)
3.1.4.1d	Configure all systems and services to permit only authorized connections.
3.1.4.1e	Manage all systems and services in a “deny by default, permit by exception” configuration for all ports, protocols, and services.
3.1.6.2	The ISO shall leverage the Agency identification and authentication framework for applications.
3.1.7.2a	Leverage the Agency identification and authentication framework for applications.
3.1.7.2b	Maintain account management capabilities (e.g., account creation, privilege configuration, maintenance, and deletion) for information systems.
3.1.7.2c	Ensure the appropriate use and warning banner is displayed by their information system.
3.1.7.2d	Establish documented rules for appropriate use and protection of information (e.g., rules of behavior).
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.2.2.3a	Allow access to information systems only to users who comply with all Agency information security awareness and training requirements.
3.2.2.3b	Ensure all personnel supporting the information system whose roles include significant information security responsibilities or elevated privileges comply with the applicable role-based information security awareness and training requirements.

3.3.2.1	The ISO shall ensure that information stored on, transmitted, or processed by their information system is protected by encryption performed in accordance with a NIST approved encryption algorithm provided through either: a. A FIPS-140-2 or FIPS-140-3 cryptographic module validated through the Cryptographic Module Validation Program (CMVP), or b. A cryptographic module approved for the protection of classified national security information. In the event that the use of encryption is technically unfeasible or would demonstrably affect the system's ability to carry out its respective mission, functions, or operations approval shall be granted in writing from the NASA CIO before an Authorizing Official may consider granting an Authorization to Operate.
3.3.3.1	The ISO shall ensure that NASA information under their control is protected by suitable encryption when in transit.
3.3.5.4	The ISO shall ensure shared resource policies, denial of service protections, boundary protection, and transmission integrity and confidentiality are implemented.
3.3.6.1	The ISO shall ensure, to the extent practicable, the separation of development and testing environment(s) from production environment(s).
3.3.7.2a	Implement data integrity protections on their information systems.
3.3.7.2b	Test information system security functions in accordance with requirements, and document the frequency and processes related to the tests.
3.4.2.2	The ISO shall implement the requirements and settings defined in all applicable standards and specifications established by the Agency Security Configuration Standards (ASCS).
3.4.3.1	The ISO shall ensure information security considerations are managed throughout their systems' development life cycle to ensure the protection of NASA information.
3.4.4.1	The ISO shall create, implement, and maintain configuration change control policies and processes for their system as needed.
3.4.5.1	ISOs shall back up user-level and system-level information.
3.4.7.4	The ISO shall be responsible for the sanitization of media and destruction of data according to policy for their information system.
3.4.8.3	The ISO shall review and update SSPs in accordance with this directive and its associated handbooks.
3.4.10.3a	Provide oversight to ensure that personnel adhere to limits on access to information and information systems.
3.4.10.3b	Manage or terminate access to secured resources following the transfer or termination of personnel.
3.4.11.3a	Ensure the completion of vulnerability and flaw remediation activities, and document and communicate residual risks, as necessary in accordance with Federal and Agency requirements.
3.4.11.3b	Ensure that software updates and patches remediating security flaws are applied to their system in accordance with Federal and Agency requirements.
3.5.2.1a	Develop, maintain, and implement risk-based maintenance policy and procedures.
3.5.2.1b	Adhere to change control and configuration management processes throughout the life cycle of their information systems.

3.5.2.1c	Maintain oversight of those authorized to perform maintenance on the components of their information system.
3.5.2.1d	Ensure that maintenance is logged for their system.
3.6.2.3a	Maintain auditing capabilities for their information system components.
3.6.2.3b	Allocate audit record storage capacity for an information system in accordance with Agency records retention requirements.
3.6.2.3c	Determine the 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.
3.6.2.3d	Ensure audit logs are 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 of the log.
3.6.2.3e	Ensure data in information systems are retained or destroyed in accordance with NASA Records Retention Schedule No 1441.1 (updated) May 18, 2020.
3.6.3.4	The ISO shall protect and sanitize media for their information system. This includes the protection of data at rest.
4.1.2.3	The ISO shall provide the CIO with a baseline of network operations and expected data flows for systems under their control.
4.2.2.2a	Ensure capabilities to continuously monitor the security posture of their information system.
4.2.2.2b	Ensure that SAISO-required cybersecurity monitoring tools are deployed to all components of their information system to collect information, and to track all events of interest.
4.2.2.2c	Develop and implement a strategy for continuous monitoring of their information system, which is consistent with the Agency strategy for continuous monitoring.
4.2.2.2d	Perform continuous monitoring of their information system and keep the AO informed of continuous monitoring results in support of the ongoing authorization of their information system, in accordance with NASA's implementation of the RMF.
4.2.3.2	The ISO shall ensure their system uses SAISO-required tools to detect malicious or unauthorized software and malicious or unauthorized changes to software or configuration.
5.2.2.3a	Designate individuals responsible for incident response reporting and management of their information system.
5.2.2.3b	Handle incident information in accordance with all data sensitivity requirements.
5.2.2.3c	Support information security investigations.

C.16 ISSO

Para #	Requirement
1.2.3.13a	Serve as the principal advisor to the ISO on issues regarding information security.
1.2.3.13b	Ensure a proper operational security posture is maintained for their information system.
1.2.3.13c	Be responsible for the day-to-day security operations of their information system.

2.3.5.4	The ISSO shall assist in the development of information security requirements for inclusion in solicitations and resulting contracts for acquisitions made in support of their information systems.
2.4.2.6a	Perform information system risk analyses in support of security control selection and tailoring, security control implementation including system configuration, and continuous monitoring.
2.4.2.6b	In collaboration with the ISO and IO(s), perform the information system security categorization, ensuring that the selected data types reflect all information generated, collected, processed and disseminated by the information system.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
4.1.2.4	The ISSO shall assist in developing event containment and remediation strategies to minimize impact to an information system.
4.2.4.4	The ISSO shall ensure that their information systems are regularly scanned for vulnerabilities or flaws that will then be remediated using SAISO-required tools, per 3.4.11.3.
5.2.2.4	The ISSO shall report all suspected or confirmed information security incidents in a timely manner.

C.17 NASA Administrator

Para #	Requirement
1.2.2.2a	Ensure the security of NASA's information and information systems.
1.2.2.2b	Ensure that NASA implements the NIST Cybersecurity Framework.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.18 NASA User

Para #	Requirement
3.1.3.3a	Use only NASA authorized and approved devices for remote access to NASA non-public information systems.
3.1.3.3b	Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely and understand the consequences for mishandling.
3.1.6.3	The NASA User shall protect identification and authentication information from unauthorized disclosure.
3.1.7.3	The NASA User shall comply with all appropriate use policies.
3.2.2.4a	Comply with applicable role-based information security and awareness training requirements.
3.2.2.4b	Acknowledge acceptance of the Agency User Rules of Behavior annually.
3.3.2.2	The NASA User shall secure and protect media under their control using access restriction and/or sanitization (in accordance with the requirements of section 3.4.7.1).
3.4.7.5	The NASA User shall mitigate the risks of leakage of non-public NASA information to unauthorized persons or entities through the sanitization of media and destruction of data according to policy.

3.6.3.2a	Protect removable media devices.
3.6.3.2b	Not use any untrusted media (as detailed in ITS-HBK-2810.11-2B).
3.6.3.2c	The NASA User shall mitigate the risks of data loss by securing and protecting media under their control, and the information contained within those devices, through the use of encryption, access restriction, and sanitization.
5.2.2.5	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).

C.19 OCSO

Para #	Requirement
1.2.3.6a	Ensure compliance with information security requirements.
1.2.3.6b	Serve as their organization's representative to the Center CISO on information security matters.
1.2.3.6c	Report the status of the organization's information security to the Center CISO and senior organization officials.
1.2.3.6d	Be an employee of the United States Federal Government.
2.4.2.3a	Verify the correct application of information system categorization criteria and requirements for their organization.
2.4.2.3b	Ensure the identification and management of common threats to their organization.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.4.7.3	The OCSO (if assigned per section 1.2.3.3) shall be responsible for the sanitization of media and destruction of data according to policy for their organization.
3.4.8.2	The OCSO (if assigned per section 1.2.3.3) shall review and update their organization's SSPs in accordance with this directive and its associated handbooks.
3.6.3.3	The OCSO (if assigned per section 1.2.3.3), in collaboration with ISOs, shall protect and sanitize media for their organization. This includes the protection of data at rest.

C.20 Officials in charge of Mission Directorates and Mission Support Offices

Para #	Requirement
1.2.2.4a	Appoint an information security point of contact to represent the mission on Agency programmatic strategic cybersecurity initiatives and serve as voting members of suitable governance bodies.
1.2.2.4b	Ensure that resources are allocated to address information and information system security requirements developed under this directive for their information systems.
1.2.2.4c	Ensure that their respective organizations, including missions, programs, projects, and institutions under their purview, comply with this directive, ensuring Operational Technology is also compliant.
1.2.2.4d	Ensure that secure software development is being practiced for NASA projects per NPR 7150.2, NASA Software Engineering Requirements.

1.2.2.4.e	Ensure that secure system development is being practiced for NASA projects per NASA specifications and standards, including NASA-STD-1006 and the NASA Cybersecurity Requirements Technical Specification.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.

C.21 Program Managers and Project Managers

C.21.1 This section includes additional resources for Program and Project Managers to assist in compliance with this directive. Additional resources are available in Appendix E.

Para #	Requirement	Related Roles	Additional Resources
1.2.3.11a	Allocate resources to protect information and information systems under their control based on an assessment of system risks.	SAISO Center CISO ISO	SSP
1.2.3.11b	Ensure identified cybersecurity risks accepted by AOs are also reflected in the program or project risk database(s)/system(s).	AO	Program/ Project Risk Database(s)/ System(s)
1.2.3.11c	Include cybersecurity as part of the program and project plans for projects (e.g., incorporate the requirements of all applicable cybersecurity standards and specifications).	SAISO Center CISO ISO	SSP
1.2.3.11d	Identify and coordinate with ISOs for information systems under their control ensuring greater integration of cybersecurity and mission personnel.	Center CIO Center CISO ISO	
1.2.3.11.e	Identify and coordinate with ISOs for information systems outside their control that support and impact their mission.	ISO	
1.2.3.11.f	Ensure that all information systems under Program Managers' and Project Managers' control are fully compliant with the requirements of this directive.	AO AODR SAISO	ATO package
2.3.3.4a	Ensure that projects or programs under their control implement the requirements of this directive.	ISO ISSO AO	ATO package
2.3.3.4b	Ensure that information security is incorporated into the planning and development of all information systems under their control by following the procedures outlined in NIST SP 800-160.	ISO ISSO	SSP Handbook ITS-HBK-2810.03-

			02B, Planning
2.4.2.7a	With the support of ISOs and ISSOs, understand and communicate to AOs any cybersecurity risks associated with any information system in a program or project under their control so that an assessment can be made of cybersecurity risk to Agency operations and resources.	ISO ISSO AO	SSP ATO package
2.4.2.7b	Verify the proper application of information system categorization criteria and requirements for the programs and projects under their control.	ISO ISSO AO	SCAR POA&M ATO package
3.1.3.2	Program Managers and Project Managers shall ensure, with respect to any information system in a program or project under their control, that all remote access is routed through authorized NASA access control points.	ISO	SSP
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.		

C.22 SAISO

Para #	Requirement
1.2.3.4a	Carry out the responsibilities delegated from the NASA CIO under FISMA (as described by section 3554(a)(3)(A) of title 44, United States Code), as well as federal and NASA Cybersecurity and Privacy Program requirements.
1.2.3.4b	Establish and maintain an office with the mission and resources to ensure compliance with federal and NASA Cybersecurity and Privacy Program requirements.
1.2.3.4c	Manage the NASA Cybersecurity and Privacy Program.
1.2.3.4d	Keep the NASA Cybersecurity and Privacy Program current with changes in the information security environment and with changes in federal policy and guidelines.
1.2.3.4e	Ensure that information security control assessments, authorizations, and OMB and FISMA reporting directives are completed across the Agency in a timely and cost-effective manner.
1.2.3.4f	Serve as the NASA CIO's primary liaison with Center CISOs, AOs, Information System Owners (ISOs), and Information System Security Officers (ISSOs).
1.2.3.4g	Oversee and arbitrate conflict resolution, relative to information security concerns, for all NASA-wide information systems.
1.2.3.4h	Ensure the planning of a framework for the use and adoption of current and new information security technologies implemented throughout the Agency.
1.2.3.4i	Maintain a process for planning, implementing, evaluating, and documenting remedial actions to address deficiencies and weaknesses in NASA's Cybersecurity and Privacy Program.
1.2.3.4j	Manage the NASA system of Record for all Assessment and Authorization artifacts, including all System Security Plans. The current System of Record is Risk Information Security Compliance System (RISCS).

1.2.3.4k	Develop, implement and manage a High Value Asset (HVA) program in accordance with Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-02.
1.2.3.4l	Develop, implement and manage a threat monitoring and incident response program, to include the NASA Security Operations Center, for NASA HVAs in accordance with Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-02.
1.2.3.4m	Be an employee of the United States Federal Government.
2.1.2.1	The NASA SAISO shall ensure the maintenance of a NASA-wide information system inventory in the NASA system of record (i.e., RISCS).
2.1.3.1	The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all physical and virtual devices and systems.
2.1.4.1	The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all software platforms and applications.
2.1.5.1	The NASA SAISO shall maintain the mapping of information system communications and data flows in the NASA system of record.
2.1.6.1	The NASA SAISO shall ensure the inventory required by section 2.1.2.1 is accurate and updated with all external information systems.
2.1.7.1	The SAISO shall consider the value of information and information systems to NASA's mission in the prioritization of information security effort and resources.
2.1.8.2a	Manage the NASA Cybersecurity and Privacy Program.
2.1.8.2b	Maintain and update, as needed to comply with federal and NASA requirements, NPD 2810.1, NPR 2810.1, and all related handbooks.
2.1.8.2c	Publish and maintain such policies, procedures, NASA Information Technology Requirements (NITRs), specifications, standards, handbooks, and memoranda as may be necessary to implement the requirements of this directive.
2.2.3.2a	Develop and maintain Agency-level information system contingency planning policies, procedures, and guidance for NASA, as coordinated through OPS.
2.2.3.2c	Ensure that Center CISOs are coordinating a Center-based information system contingency program.
2.2.3.2d	Establish recovery metrics and objectives for information systems.
2.3.2.1a	Develop and document a NASA-wide NASA Cybersecurity and Privacy Program that includes an overview and descriptions of measures of performance, enterprise information security architecture, critical infrastructure, risk management strategy, and an information security assessment and authorization process.
2.3.2.1b	Provision a NASA-wide repository for information security documentation.
2.3.2.1c	Review, update, and augment the NASA Cybersecurity and Privacy Program.
2.3.2.1d	Ensure that the NASA Cybersecurity and Privacy Program plan, policy, and requirements are implemented.
2.3.2.1e	Update and disseminate Organization Defined Values via a cybersecurity specification updated at least annually.
2.3.2.1f	Define a process for the development, documentation, and maintenance of plans of action and milestones (POA&M) and for the acceptance of risk.
2.3.2.1g	With respect to unclassified information systems, be responsible for ensuring NASA's implementation of the NIST RMF.

2.3.3.2	Coordinate information security compliance with internal and external resources across the Agency.
2.3.3.2a	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).
2.3.3.2b	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.
2.3.4.1a	Comply with OMB and FISMA reporting requirements.
2.3.4.1b	Fulfill OMB and FISMA contingency plan testing requirements.
2.3.5.2a	Report to the NASA Administrator on the effectiveness of NASA's Cybersecurity and Privacy Program, including the progress of remedial actions, as required by FISMA.
2.3.5.2b	Include information security resource requirements in programming and budgeting documentation.
2.4.2.1a	Identify and manage common cybersecurity threats to NASA.
2.4.2.1b	Consistent with NPR 8000.4, define and make available an RMF that describes a uniform methodology for risk assessment that applies to all Agency internal and external systems.
2.4.2.1c	Ensure the assessment, updating, and dissemination of information regarding Agency Common Controls.
2.4.2.1d	Ensure the assessment, updating, and dissemination of information regarding those portions of Hybrid Controls that the Agency implements.
2.4.2.1e	Manage the NASA-wide information security performance metrics program.
2.4.2.1f	Work with the applicable Information Sharing and Analysis Centers (ISACs) and other relevant information sharing fora.
2.5.2.1	The SAISO shall develop and implement a Cybersecurity Risk Management Strategy, which includes:
2.5.2.1a	Definition of NASA’s risk management priorities and constraints for NASA high-value assets and mission and institutional systems.
2.5.2.1b	Documentation criteria as a basis for determination of NASA’s risk tolerances and assumptions.
2.5.2.1c	Description of the importance of accurate and timely assessment of the likelihood and consequence severity of threats to NASA’s critical infrastructure within the unique threat environment for NASA operations.
2.5.2.1d	Ensure the underlying basis for risk acceptance decisions by AOs across NASA conform to validated practices set forth in NPR 8000.4.
2.6.2.1a	In awareness of Office of Safety and Mission Assurance roles, develop, manage, and update NASA’s Cyber SCRM process.
2.6.2.1b	Identify, prioritize, and assess suppliers and third-party partners of information systems using a cyber supply chain risk assessment process.
2.6.2.1c	Work with program and procurement officials in NASA to ensure that:
2.6.2.1c.(1)	Contracts with suppliers and third-party partners implement measures designed to meet the objectives of this directive and the Cyber SCRM process required by section 2.6.2.1a.

2.6.2.1c.(2)	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
2.6.2.1c.(3)	Response and recovery planning and testing are conducted with suppliers and third-party providers.
3.1.5.1	The SAISO shall ensure that NASA maintains a Network Access Control Policy to monitor, control, prevent, or regulate device and system access to NASA networks.
3.1.7.1a	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 consent banner.
3.1.7.1b	Ensure that the NASA consent disclaimer requirements for internal systems are met through the display of the appropriate use and consent banner statements.
3.2.2.1	All NASA officials listed in section 1.2 (relating to Roles and Responsibilities) shall complete any role-based training activities required of their position.
3.2.2.2a	Develop, maintain, and promote NASA-wide information security awareness and training.
3.2.2.2b	Define and make available all Agency information 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, and others.
3.2.2.2c	Define educational courses and materials that can be used to satisfy Agency information security awareness and training requirements.
3.2.2.2d	Oversee the fulfillment of training requirements across the Agency and for external stakeholders, to include tracking and reporting on the completion of information security awareness and training requirements in the Agency system of record.
3.2.2.2e	Maintain the NASA User Rules of Behavior and track user annual acceptance.
3.3.5.2	The SAISO shall ensure the provision of Center-level boundary protection for systems that share a common infrastructure or services.
3.3.7.1a	Ensure that the capabilities 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).
3.3.7.1b	Ensure that data is protected against unauthorized access, tampering, alteration, loss, and destruction.
3.4.2.1a	Create and maintain processes for development, approval, distribution, and verification of information security configuration baselines for covered articles, incorporating, for example, the concept of least functionality.
3.4.2.1b	Create and maintain processes to monitor information security baseline configuration compliance.
3.4.2.1c	Ensure information security baseline configurations conform to federal guidelines and requirements.
3.4.6.1	The SAISO shall coordinate with OPS to ensure the development and maintenance standards and guidance for security of NASA information systems' physical operating environments.
3.4.8.1	The SAISO shall identify, implement, and maintain a NASA-wide resource for the management of corrective action plans to mitigate information system security weaknesses.

3.4.9	The SAISO shall ensure that the effectiveness of protection technology (e.g. continuous monitoring tools) is measured and shared to improve NASA's information security posture.
3.4.10.1	The SAISO shall make all offices aware of requirements and expectations related to ICAM.
3.4.11.1a	Develop and maintain a Vulnerability Management Plan.
3.4.11.1b	Establish processes and systems for the management of vulnerability, flaw remediation, and information system monitoring.
3.4.11.1c	Ensure the proper handling of vulnerability and 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.
3.6.2.2a	Maintain Agency information system record retention policies for logs, and minimum auditable events.
3.6.2.2b	Develop and maintain log information security auditing capabilities for NASA information system logs.
4.1.2.2a	Ensure the capability to detect anomalous events on NASA information systems and networks.
4.1.2.2b	Establish procedures for detecting, analyzing, and responding to anomalous events.
4.2.2.1a	Develop and implement a strategy for continuous monitoring of NASA information systems.
4.2.2.1b	Define the acceptability, and requirements for use, of cybersecurity monitoring tools for use across the agency.
4.2.3.1a	Define requirements for tools to detect malicious or unauthorized software and malicious or unauthorized changes to software or configuration.
4.2.3.1b	Ensure such detection capability extends to mobile devices having access to NASA networks.
4.2.4.1a	Define requirements for tools to scan NASA information systems for vulnerabilities.
4.2.4.1b	Regularly review and approve the use of Agency tools for vulnerability scanning.
4.3.2.1a	Ensure that detection processes and procedures comply with all requirements (e.g., law, regulations, guidance, or other NASA NPDs and NPRs).
4.3.2.1b	Establish a process to test and continuously improve detection processes and procedures.
5.1.2.2a	Implement and manage a NASA-wide SOC.
5.1.2.2b	Designate an Agency Incident Response Manager for cybersecurity incidents.
5.1.2.2c	Develop and maintain a NASA-wide Incident Response Plan, which shall contain processes and procedures for detecting, reporting, analyzing, and responding to information security incidents.
5.1.2.2d	Oversee all activities related to incident response and management.
5.2.2.1a	Include elements providing for coordination with internal and external stakeholders (e.g., external support from law enforcement agencies) in the incident response plan required by section 5.1.2.2c.
5.2.2.1b	Support investigations into information security incidents related to criminal activity, counterintelligence, or counterterrorism.

5.2.2.1c	Support investigations into information security incidents initiated by the Office of the General Counsel, the Office of Chief Human Capital Officer, a Center's Office of Human Resources, and a Center's Office of the Chief Counsel.
5.2.2.1d	Refer any suspected criminal, counterintelligence, or counterterrorism activity to the OIG and OPS.
5.2.2.1e	Ensure that incidents are reported to external agencies as directed by laws and regulations.
5.3.2.1	The SAISO shall include elements in the Incident Response Plan that provide for analysis of information security incidents as required by section 5.1.2.2c.
5.4.2.1	The SAISO shall include elements that provide for containment and mitigation of information security incidents in the Incident Response Plan required by section 5.1.2.2c.
5.5.2.1	The SAISO shall incorporate lessons learned from current or prior information security incidents in the Incident Response Plan required by section 5.1.2.2c.
6.1.2.1	The SAISO shall develop and maintain a NASA-wide Incident Recovery Plan, which contains processes and procedures for incorporating lessons learned from incident response activities. The Incident Recovery Plan may be executed during or after information security incidents and may be included in the Incident Response Plan.
6.2.2.1	The SAISO shall incorporate lessons learned from current or prior incidents in the Incident Recovery Plan required by section 6.1.2.1.
6.3.2.1	The SAISO shall ensure the plan required by section 6.1.2.1 includes:
6.3.2.1a	A public relations management strategy that works to restore trust in NASA's mission capabilities.
6.3.2.1b	Procedures for communications with internal and external stakeholders as well as executive and management teams.
2.2.3.2b	Develop and test information security contingency plans in place to continue fulfilling the business functions of NASA in support of the Agency's mission essential functions.
6.3.2.1	The SAISO shall ensure the plan required by section 6.1.2.1 includes:

Appendix D References

D.1 Office of Management and Budget (OMB) Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003.

D.2 OMB Memorandum M-0524, Implementation of Homeland Security Directive (HSPD) 12.

D.3 OMB Memorandum M-06-16, Protection of Sensitive Agency Information.

D.4 NPD 1600.2 NASA Security Policy.

D.5 NPD 1600.3, Policy on Prevention of and Response to Workplace Violence.

D.6 NPR 1040, NASA Continuity of Operations Planning (COOP) Procedural Requirements.

D.7 NPR 1382, NASA Privacy Procedural Requirements.

D.8 NPR 1620.2, Physical Security Vulnerability.

D.9 NPR 1620.3, Physical Security Requirements for NASA Facilities and Property.

D.10 NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

D.11 NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

D.12 NPR 7123.1, NASA Systems Engineering Processes and Requirements.

D.13 NPR 7150.2, NASA Software Engineering Requirements.

D.14 NPR 8831.2, Facilities Maintenance and Operation Management.

D.15 HSPD-20, National Continuity Policy, May 2007.

D.16 NIST SP 800-21, Guideline for Implementing Cryptography in the Federal Government.

D.17 NIST SP 800-30, Risk Management Guide for Information Technology Systems.

D.18 NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

D.19 NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.

D.20 NIST SP 800-55, Performance Measurement Guide for Information Security.

D.21 NIST SP 800-58, Security Considerations for. Voice Over IP Systems.

D.22 NIST SP 800-61, Computer Security Incident Handling Guide.

D.23 NIST SP 800-63, Electronic Authentication Guideline. NIST SP 800-64, Security Considerations in the System Development Life Cycle.

D.24 NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.

D.25 NIST SP 800-83, Guide to Malware Incident Prevention and Handling.

D.26 NIST SP 800-88, Guidelines for Media Sanitization.

D.27 NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

D.28 NIST SP 800-171, Protecting Controlled Unclassified Information.

D.29 X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Federal Public Key Infrastructure Policy Authority.

D.30 FIPS Publication 140-2, Security Requirements for Cryptographic Modules.

D.31 FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

D.32 FIPS Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

Appendix E Requirements Matrix with respect to system lifecycle

E.1 Overview

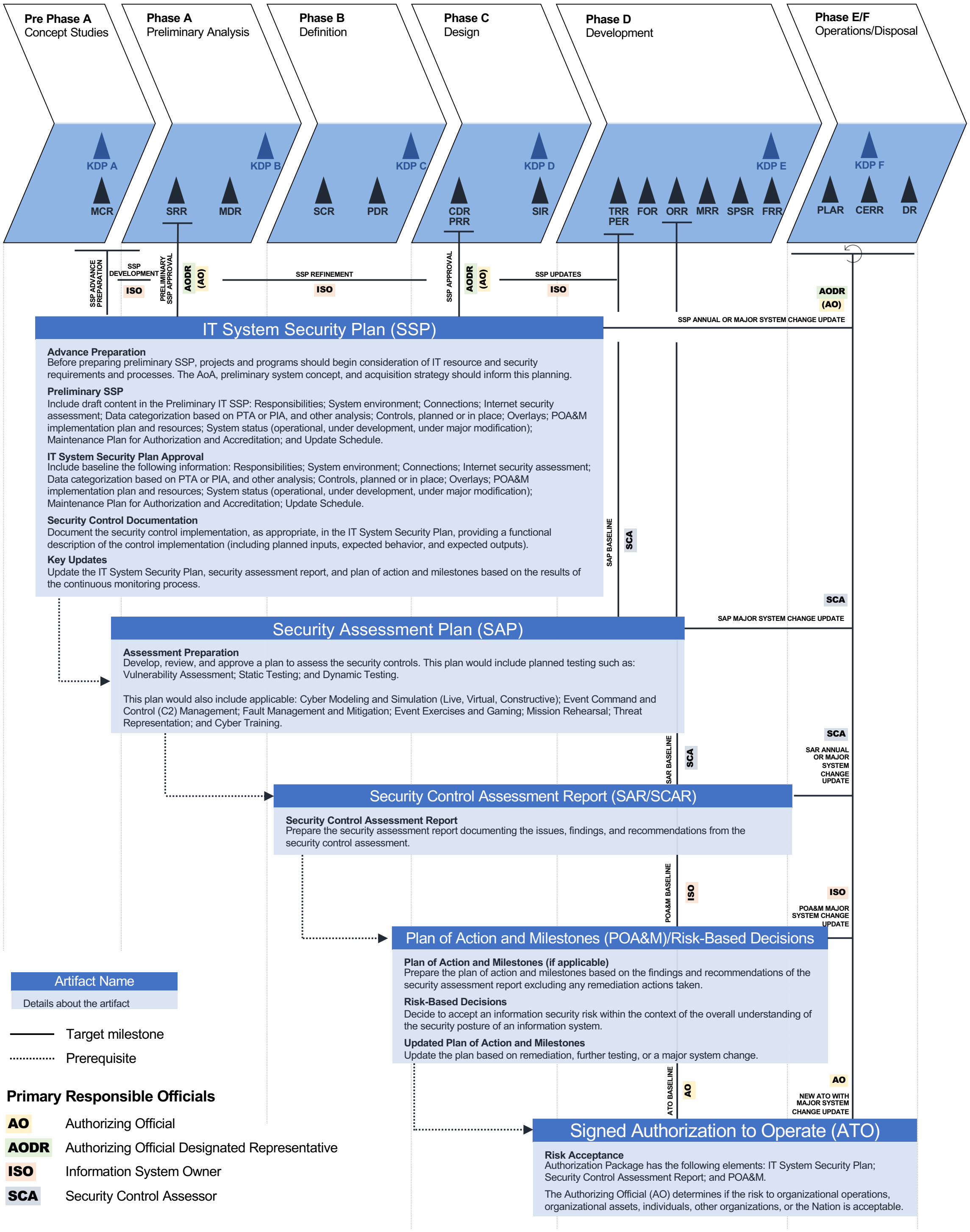
E.1.1 This appendix provides an overview of information security artifacts and processes mapped to stages in the NPR 7120 project and program development life cycle.

E.1.2 This appendix is included to provide information regarding the application of information security principles and the requirements this directive in the context of programs and projects primarily governed by the NPR 7120 lifecycles.

E.1.3 Given the wide range of projects and activities, the timelines and artifacts outlined in this appendix are to be regarded as informative rather than restrictive.

E.1.4 Figure E-1 provides a visual representation of the information security artifacts related to the program or project lifecycle.

Information Security Artifacts in the System Development Lifecycle



IT System Security Plan (SSP)

Advance Preparation
Before preparing preliminary SSP, projects and programs should begin consideration of IT resource and security requirements and processes. The AoA, preliminary system concept, and acquisition strategy should inform this planning.

Preliminary SSP
Include draft content in the Preliminary IT SSP: Responsibilities; System environment; Connections; Internet security assessment; Data categorization based on PTA or PIA, and other analysis; Controls, planned or in place; Overlays; POA&M implementation plan and resources; System status (operational, under development, under major modification); Maintenance Plan for Authorization and Accreditation; and Update Schedule.

IT System Security Plan Approval
Include baseline the following information: Responsibilities; System environment; Connections; Internet security assessment; Data categorization based on PTA or PIA, and other analysis; Controls, planned or in place; Overlays; POA&M implementation plan and resources; System status (operational, under development, under major modification); Maintenance Plan for Authorization and Accreditation; Update Schedule.

Security Control Documentation
Document the security control implementation, as appropriate, in the IT System Security Plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

Key Updates
Update the IT System Security Plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Security Assessment Plan (SAP)

Assessment Preparation
Develop, review, and approve a plan to assess the security controls. This plan would include planned testing such as: Vulnerability Assessment; Static Testing; and Dynamic Testing.

This plan would also include applicable: Cyber Modeling and Simulation (Live, Virtual, Constructive); Event Command and Control (C2) Management; Fault Management and Mitigation; Event Exercises and Gaming; Mission Rehearsal; Threat Representation; and Cyber Training.

Security Control Assessment Report (SAR/SCAR)

Security Control Assessment Report
Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

Plan of Action and Milestones (POA&M)/Risk-Based Decisions

Plan of Action and Milestones (if applicable)
Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

Risk-Based Decisions
Decide to accept an information security risk within the context of the overall understanding of the security posture of an information system.

Updated Plan of Action and Milestones
Update the plan based on remediation, further testing, or a major system change.

Signed Authorization to Operate (ATO)

Risk Acceptance
Authorization Package has the following elements: IT System Security Plan; Security Control Assessment Report; and POA&M.

The Authorizing Official (AO) determines if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

Artifact Name

Details about the artifact

——— Target milestone

········ Prerequisite

Primary Responsible Officials

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ISO	Information System Owner
SCA	Security Control Assessor

Figure E-1. Mapping of artifacts to stages of the NPR 7120 life cycle

E.2 IT System Security Plan

E.2.1 Overview

(1) The SSP is the critical cybersecurity plan for information systems in any given project or program. It addresses the threats and associated risks faced by the system as provided in section 2.3.5.3. This is the primary artifact that will define cybersecurity risk and processes throughout the life of an information system. This artifact and the information system are registered with the OCIO in the Risk Information Security Compliance System (RISCS).

(2) The AO or the AODR has primary responsibility for the approving the SSP, but the ISO prepares the plan. Supporting roles include the CIO, SAISO, and IO, and ISSO.

(3) The Program or Project Manager's role is to ensure adequate planning (to include resource planning) and effort is applied to this vital document and associated processes per sections 1.2.3.11a, 2.3.3.4a, and 2.4.2.7b.

E.2.2 Advance preparation

(1) Before preparing preliminary SSP, projects and programs should begin consideration of IT resource and security requirements and processes. The Analysis of Alternatives (AoA), preliminary system concept, and acquisition strategy should inform this planning.

(2) In general, the system concept development, including preliminary IT requirements are reviewed at SRR. Information useful at this stage includes:

(a) network diagram;

(b) data flows; and

(3) system interconnections.

E.2.3 Preliminary SSP

(1) In general, at MDR a preliminary SSP is provided.

(2) Examples of items in the Preliminary IT SSP include:

(a) Responsibilities;

(b) System environment;

(c) Connections;

(d) Internet security assessment;

(e) Data categorization based on Information and Privacy Threshold Analysis (IPTA) or Privacy Impact Assessment (PIA), and other analysis;

(f) Controls, planned or in place;

(g) Overlays;

(h) POA&M implementation plan and resources;

(i) System status (operational, under development, under major modification);

(j) Maintenance Plan for Authorization and Accreditation; and

(k) Update Schedule.

E.2.4 IT System Security Plan Approval

(1) In general, at PDR the AO or AODR approves the SSP.

(2) The approval package includes the following information:

(a) Responsibilities;

(b) System environment;

(c) Connections;

(d) Internet security assessment;

(e) Data categorization based on IPTA or PIA, and other analysis;

(f) Controls, planned or in place;

(g) Overlays;

(h) Plan of Action and Milestones (POAM) implementation plan and resources;

(i) System status (operational, under development, under major modification);

(j) Maintenance Plan for Authorization and Accreditation; and

(k) Update Schedule.

E.2.5 Security Control Documentation

(1) Document the security control implementation, as necessary, in the IT System Security Plan, providing a functional description of the control implementation, including:

(a) planned inputs;

(b) expected behavior; and

(c) expected outputs.

E.2.6 Key Updates

(1) Update the IT System Security Plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

E.3 Security Assessment Plan

E.3.1 Overview

(1) The primary way that an authorizing official can assess mitigated and residual risks is the results of testing the security controls described in the Security Assessment Plan (SAP). The testing described in this plan will identify vulnerabilities as well as confirm adequate implementation of the security controls. Like other test plans, this is evaluated in the Test Readiness Review (TRR).

(2) The Security Control Assessor has primary responsibility for the SAATP. Supporting roles include the AO, AODR, CIO, SAISO, ISO, ISSO, and IO.

(3) The Program or Project Manager's role is to ensure test planning and testing are conducted.

E.3.2 Assessment Preparation

(1) Develop, review, and approve a plan to assess the security controls. This plan would include planned testing such as:

(a) Vulnerability Assessment;

(b) Static Testing; and

(c) Dynamic Testing.

(2) This plan would also include:

(a) Cyber Modeling and Simulation (Live, Virtual, Constructive);

(b) Event Command and Control (C2) Management;

(c) Fault Management and Mitigation;

(d) Event Exercises and Gaming;

(e) Mission Rehearsal;

(f) Threat Representation; and

(g) Cyber Training.

E.4 Security Control Assessment Report(s)

E.4.1 Overview

(1) The Security Control Assessment Report (SAR/SCAR) documents the results of the testing performed, particularly highlighting vulnerabilities remaining in the information system.

(2) The Security Control Assessor has primary responsibility for the SAR/SCAR. Supporting roles include the ISO and ISSO.

(3) The Program or Project Manager will submit SAR/SCAR along with a plan or action to remediate remaining vulnerabilities as part of their ATO package to receive an Authorization to Operate.

E.4.2 Security Control Assessment Report

(1) In general, at ORR the SAR/SCAR is prepared.

(2) The SAR/SCAR documents the issues, findings, and recommendations from the security control assessment.

E.4.3 SAR/SCAR Update

(1) The SCAR is updated annually or with major system changes upon conclusion of further system testing.

E.5 Plan of Action and Milestones/Risk-Based Decisions

E.5.1 Overview

(1) A POA&M identifies plans to remediate any documented information security deficiencies or vulnerability in an information system. Depending on the criticality of the deficiency or vulnerability, an AO is unlikely to give Authorization to Operate until elements of this plan are complete.

(2) The ISO has primary responsibility for the POA&M under sections 2.4.2.5b and c. Supporting roles include the ISSO and the IO.

(3) The Program or Project Manager's role in the POA&M process is to ensure the actions required in this plan are incorporated into overall project plans and tracked to completion as well as to ensure accepted risks are captured in the Project Risk database.

E.5.2 Plan of Action and Milestones (if applicable)

(1) In general, at Operational Readiness Review (ORR) the plan of action and milestones is prepared.

(2) The POA&M is based on the findings and recommendations in the security assessment report excluding any remediation actions taken.

E.5.3 Risk-Based Decisions

(1) Decide to accept an information security risk within the context of the overall understanding of the security posture of an information system.

E.5.4 Updated Plan of Action and Milestones

(1) Update the plan based on remediation, further testing, or a major system change.

E.6 Authorization to Operate

E.6.1 Overview

(1) A signed ATO is required for operation of an information system under section 2.4.2.5i. This signature is final confirmation that the AO considers that risks are adequately mitigated and the residual risk to Mission operations and Agency personnel is acceptable compared with the value of operating the information system.

(2) The AO has responsibility to approve the ATO package under section 1.2.3.8a, and the AO may not delegate this responsibility (see section 1.2.3.8c). The AODR and SAISO play supporting roles in the approval process of an ATO.

(3) Approval of this package is the Program or Project Manager's primary indication that a system under their control is compliant with this directive under section 1.2.3.11c. The PM role in the ATO process is to ensure the project team has prepared a complete authorization package that correctly identifies the state of information system described.

E.6.2 Risk Acceptance

(1) ATO package has the following elements:

(a) IT System Security Plan;

(b) Security Control Assessment Report(s); and

(c) POA&Ms and risk-based decisions.

(2) The AO determines if the cybersecurity risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.