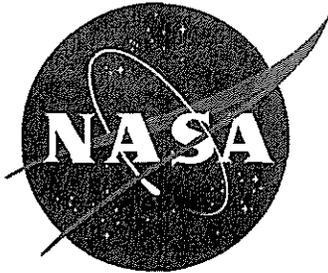


NASA Information Technology Requirement



NITR-2810-23

Effective Date: March 1, 2009

Expiration Date: May 16, 2011

NASA Authorizing Official (AO) Procedural Requirements

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

P.5 MEASUREMENT AND VERIFICATION

P.6 CANCELLATION

CHAPTER 1. Authorizing Official Policy and Procedures

1.1 AO Information Security Requirements

1.2 AO Roles and Responsibilities

APPENDIX A. Definitions

APPENDIX B. Acronyms

DISTRIBUTION:

NODIS

Change History

NITR-2810-23, NASA Authorizing Official Procedural Requirements

Change Number	Date	Change Description

PREFACE

P.1 PURPOSE

This NASA Information Technology Requirement (NITR) describes the NASA Authorizing Official (AO) policy and procedures for NASA information and information systems to meet the requirements of Public law, the National Institute of Standards and Technology (NIST), and the Agency mission.

P.2 APPLICABILITY

This NITR applies to unclassified information and information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

P.3 AUTHORITY

Reference Paragraph P.3, NPR 2810.1, Security of Information Technology.

P.4 APPLICABLE DOCUMENTS

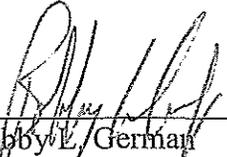
- a. NPR 2810.1, Security of Information Technology.
- b. NPR 1600.1, NASA Security Program Procedural Requirements.
- c. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- d. NIST Special Publication (SP) 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- e. NIST SP 800-53, Guide for Assessing the Security Controls in Federal Information Systems.
- f. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.
- g. 44 U.S.C. 3535, Federal Information Security Management Act (FISMA) of 2002.
- h. NPD 2810.1, NASA Information Security Policy.

P.5 MEASUREMENT AND VERIFICATION

None

P.6 CANCELLATION

The next version of NPR 2810.1 cancels this NITR.



Bobby L. German
Chief Information Officer (Acting)

3/1/09

Date

CHAPTER 1. Authorizing Official Policy and Procedures

1.1 AO Information Security Requirements

1.1.1 The NASA AO shall:

- a. Be a senior NASA official with the authority to formally assume the responsibility for operating an information system at an acceptable level of risk to NASA operations, Agency assets, or individuals; and
- b. Through security accreditation, assume responsibility and accountability for the risks accepted with operating the information system.

1.1.1.1 These responsibilities shall include, but are not limited, to that specified in:

- a. 44 U.S.C. 3544, Federal Information Security Management Act (FISMA) of 2002;
- b. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems; and
- c. NPR 2810.1, Security of Information Technology.

1.1.2 The AO shall have inherent U.S. government authority and, as such, must be a government employee.

1.1.3 The AO shall be approved by the NASA CIO before assuming AO responsibilities and authority.

1.1.4 The AO shall not be the information system Program/Project Manager or an individual directly responsible for implementing or evaluating the system security controls (e.g., the Information System Security Officer (ISSO), Computer Security Official (CSO), or Certification Agent (CA) for the system).

1.1.5 When the AO changes, the new AO shall become knowledgeable of the system risks, accept the risks for the Agency, and review the system security plans and the system Plan of Action and Milestones (POA&Ms).

1.1.5.1 Unless directed by the new AO, re-accreditation shall not be required as the result of an AO change.

1.1.6 Due to the breadth of responsibilities and significant demands on time, an AO cannot always be expected to participate directly in the planning and technical meetings that occur during the security certification and accreditation process. An Authorizing Official Designated Representative (AODR) may be designated to support the AO in certification and accreditation (C&A) security control assessment activities and responsibilities in accordance with NIST SP 800-37.

1.1.6.1 The AODR shall be an individual acting on the AO's behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

1.1.6.2 The AODR designation by the AO shall be in writing, identify the empowerment granted, and signed by the AO.

1.1.6.3 The only activity that shall not be delegated by the AO is the security accreditation decision and the signing of the associated accreditation decision letter.

1.1.6.4 When an AODR is not selected, the AO shall be responsible for carrying out the AO activities as required by NIST 800-37, Guide for Security Certification and Accreditation of Federal Information Systems; and NPR 2810.1, Security of Information Technology.

1.1.7 The NASA AOs by Agency position are identified in Table 1-1:

If the System is,	Then the Authorizing Official is the
Office Automation of Information Technology (OAIT)	NASA Deputy CIO
Program Unique – A system funded by a single Mission Directorate or Mission Support Office	Deputy Associate Administrator for the Mission Directorate or Mission Support Office funding the system. The Deputy Associate Administrator may recommend a senior executive located at the hosting Center as the AO if the individual meets the AO Roles and Responsibilities requirements as specified of NIST SP 800-37, including the budgetary oversight of the information system.
A Multi-funded system (majority funded by single Mission Directorate or Mission Support Office)	Deputy Associate Administrator for the Mission Directorate or Mission Support Office funding the majority of the system. The Deputy Associate Administrator may recommend a senior executive located at the hosting Center as the AO if the individual meets the AO Roles and Responsibilities requirements as specified of NIST SP 800-37, including the budgetary oversight of the information system.
A Multi-funded system (no majority Mission Directorate funding)	Appropriate Deputy Center Director Directorate
A Center funded and managed system	Deputy Center Director
Institutions and Management's Responsibility	Deputy Assistant Administrator for the Appropriate Functional Area
For the Office of Inspector General (OIG)	NASA Deputy Inspector General (IG)
For Office of Safety and Mission Assurance	Deputy Chief Safety and Mission Assurance
For the Chief Engineer	Deputy Chief Engineer

If the System is,	Then the Authorizing Official is the
For the Office Strategic Communications	Deputy Assistant Administrator for Strategic Communications
For Office of the Chief Financial Officer (OCFO)	Deputy Chief Financial Officer (CFO)
For Office of Program Analysis and Evaluation	Deputy Associate Administrator for Program Analysis and Evaluation
For the Office of Program and Institutional Integration	Deputy Director Program and Institutional Integration
For Office of the Chief Information Officer	Deputy Chief Information Officer
For Office of Security and Program Protection	Deputy Assistant Administrator for Security and Program Protection
For Office of the Chief Health and Medical Officer	Chief Health and Medical Officer
For Office of External Relations	Deputy Assistant Administrator for External Relations
For Office of the General Council	Deputy General Council
For the Office of Innovative Partnership Program	Deputy Director Innovative Partnership Program

Table 1-1. Authorizing Officials

1.2 AO Roles and Responsibilities

1.2.1. The AO shall:

- a. Formally assume the responsibility for operating an information system at an acceptable level of risk to Agency/Center operations, Agency/Center assets, or individuals.
- b. Oversee the budget and business operations of the information system within the Agency/Center.
- c. Accept the system security plan, as well as the determination of risk to Agency/Center operations, Agency/Center, and individuals.
- d. Approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding.
- e. Make decisions with regard to the planning and resourcing of the security certification and accreditation activities.
- f. Assume responsibility and accountability for the risks associated with operating the information system(s).
- g. Issue an interim authorization to operate (IATO) (or a limited authority to operate) the information system with specific time, terms and conditions for operations; or deny authorization to operate (DATO) the information system (or if the system is already operational, halt operations) if unacceptable security risks exist.

h. Ensure the C&A process is performed during life cycle changes of systems, when a significant change is determined to affect security, and at least every three years prior to the expiration of the last C&A.

i. Ensure that the C&A process is followed prior to granting a full Authorization to Operate (ATO) or an IATO. This includes when a significant change is determined to affect security and at least every three years prior to the expiration of the last C&A.

j. Advocate that funding be directed and/or redirected to implement security controls required to achieve full ATO.

k. Determine when there has been a significant change to the information system that requires re-accreditation.

1.2.2. AODR shall:

1.2.2.1. Act on the AO's behalf in coordinating and carrying out the necessary activities required during the security C&A of an information system.

1.2.2.2. As empowered in writing by the AO, the AODR shall:

a. Make decisions with regard to the planning and resourcing of the security C&A activities, the acceptance of the system security plan, and the determination of risk to Agency/Center operations, Agency/Center assets, and individuals.

b. Interact with the Senior Agency Information Security Officer (SAISO), Center Information Technology Security Manager (ITSM), Information System Owner (ISO), ISSO, CA, user representative(s), and other interested parties during the security C&A process.

c. Assist the AO in meeting the information security requirements of Federal law, NIST guidelines, and Agency policy.

1.2.3. NASA Chief Information Officer (CIO)

1.2.3.1. The NASA CIO shall be the approval authority for all Agency AO who have the authority to formally assume the system risk to Agency operations and who meet the requirements of paragraph 1.1 above.

APPENDIX A. Definitions

Term	Definition
Authorizing Official	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200 adapted]
Authorizing Official Designated Representative	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Certification	A confirmation in formal documentation that an accepted standard has been met.
Certification Agent	The individual, group, or organization responsible for conducting security certification.
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST; CNSS 4009, Adapted)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502] (Also referred to as IT System)
Information System Security Officer	Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [Committee for National Security Systems (CNSS) Inst. 4009, Adapted]
Information Technology	Any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Agency. [FAR 2.101]
Information Technology Security Manager	NASA Center Senior Information Security Officer responsible for assisting the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws, directives, policies, standards, and guidelines and compliance with the FISMA

	section 3541 et seq..
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation [FIPS 199]
Plan of Action and Milestones (POA&M) - Programmatic	A Programmatic POA&M is used to document and track the security deficiencies and/or weaknesses in the security controls of an IT system, multiple IT systems, and/or organizational level policies, programs, and C&A implementation and the documentation and tracking of the mitigation of these deficiencies. These deficiencies are normally identified from audits/investigations by the OIG, Government Accounting Office (GAO) (congressional), or other authorized agency. A programmatic POA&M shall be managed and tracked at the Agency level and with mitigation reports provided to the agency/organization that identified the deficiency
Plan of Action and Milestones (POA&M) - System	A System POA&M is used to document the security deficiencies and/or weaknesses in the security controls of an IT system and to track the mitigation of those deficiencies. These deficiencies are normally identified from the system security control assessments, security impact analyses, and continuous monitoring activities. A POA&M shall be prepared/established for every information system that has a deficiency
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]

APPENDIX B. Acronyms

AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
CA	Certification Agent
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CSO	Computer Security Official
DATO	Deny Authorization to Operate
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IATO	Interim Authorization to Operate
ISO	Information System Owner
ISSO	Information System Security Officer
ITSM	Information Technology Security Manager
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OAIT	Office Automation of Information Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SP	Special Publication