

NASA Information Technology Requirement

NITR-2830-1

Effective Date: January 5, 2009

Expiration Date: February 9, 2011

**Networks in NASA Internet Protocol (IP) Space or NASA Physical
Space**

Responsible Office: OCIO/ Chief Information Officer

Table of Contents

Change History

PREFACE

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 CANCELLATION

1.0 Requirements for Networks in NASA IP Space or NASA Physical Space

- 1.1 Requirement
- 1.2 Responsibilities
- 1.3 Waivers

Appendix A Definitions

Appendix B Acronyms

Distribution

NODIS

Center Chief Information Officers

Change History

NITR-2830-1, Networks in NASA Internet Protocol (IP) Space or NASA Physical Space

Change Number	Date	Change Description

PREFACE

P.1 PURPOSE

a. The purpose of this NASA Information Technology Requirement (NITR) is to establish requirements regarding networks residing on or within NASA physical space or Internet Protocol (IP) space.

P.2 APPLICABILITY

a. This NITR is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers, as well as IP networks on, within, or off of NASA physical or logical IP space or physically located on NASA facilities. It applies to the NASA Jet Propulsion Laboratory to the extent specified in their contract. An IP network is defined, for the purposes of this policy, as any collection of devices communicating over a wired or wireless network using IP-based technologies. For the purpose of this document a system consists of a device or devices that share an accreditation boundary.

P.3 AUTHORITY

a. Same as NPR 2830.1.

b. Per NASA Policy Directive (NPD) 2800.1B, the NASA Chief Information Officer (CIO) has the responsibility, accountability and authority to 1) manage the NASA IT infrastructure as an integrated end-to-end service to improve security, efficiency, and inter- Center collaboration; 2) develop and enforce applicable Agency policies, procedures, standards, models, documents and guidance that define the NASA IT environment; and 3) ensure the appropriate confidentiality, integrity and availability of information residing on, or processed by, NASA's automated information systems through implementation and enforcement of risk-based policies, procedures, standards, guidelines, control techniques, and training mechanisms.

P.4 APPLICABLE DOCUMENTS

a. NPD 2800.1, Management of Information Technology.

b. NPR 2830.1, NASA Enterprise Architecture.

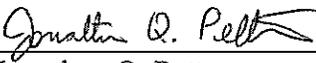
c. NPR 2810.1, Security of Information Technology.

P.5 MEASUREMENT AND VERIFICATION

a. None

P.6 CANCELLATION

a. The next version of NPR 2830.1 cancels this NITR.


Jonathan Q. Pettus
Chief Information Officer

1 - 5 - 09
Date

1.0 Requirements for Networks in NASA IP Space or NASA Physical Space

1.1 Requirement

1.1.1 In maintaining the integrity of NASA's network infrastructure architecture and security accreditation boundary, the following requirements shall be administered:

- a. Internet Protocol (IP) address space that has been registered, allocated and assigned to NASA, shall only be used to service NASA systems and networks within the accreditation boundary. Sharing, transferring, allocating, assigning or using NASA IP address space or a subnet off of NASA IP address space with any non-NASA systems or networks is prohibited.
- b. The construction and establishment of any non-NASA system or network within the NASA accreditation boundary and furnished property is prohibited. A non-NASA system or network is any system or network that is not necessary to the performance of a NASA contract and to which NASA does not have title to the system or network. This does not apply to personal devices such as cell phones or personal digital Assistants (PDA) that connect to outside networks (e.g. commercial cellular networks), are not networked within the NASA furnished property, and that have no connectivity to systems or networks in NASA IP address space.
- c. Exception to the use of NASA IP address space with any non-NASA systems or networks is the use of individual workstations on the NASA Headquarters and Center Guest Networks where the Guest Network has a defined accreditation boundary, is accredited with an authority to operate, and the Guest Network has no connection to other NASA systems or networks that use NASA IP address space.

1.2 Responsibilities

1.2.1 Center CIOs shall:

- a. Be responsible for ensuring compliance with this NITR and for ensuring that all non-compliant networks transition to a compliant state by January 1, 2009, or are operating under an approved waiver.
- b. Approve all waiver requests from their Center activities and from cognizant Center contractors.
- c. Submit the Center CIO approved waiver request to the Agency CIO through the Senior Agency Information Security Officer (SAISO).

1.2.2 The Center Information Technology Security Manager (ITSM) shall provide oversight and support for:

- a. The development and tracking of Center processes for compliance with this NITR in support of the Center CIO.
- b. The preparation, tracking, and IT security technical support for waiver requests.

1.2.3 The NASA CIO shall be the final approval authority for all waivers to this requirement.

1.2.4 The NASA SAISO shall:

- a. Provide the Agency CIO tracking and control for waiver requests.

b. Provide the Agency staffing and recommendation to the Agency CIO for the waiver request.

1.3 Waivers

1.3.1 Waivers shall be submitted in accordance with Appendix C, Information Technology (IT) Waiver Process.

1.3.1.1 If the waiver includes, or results in, an unmitigated security weakness of a NASA information or information system or network, a Plan of Action and Milestones (POA&M) shall be prepared, approved and documented in the System Security Plan (SSP) in accordance with Agency requirements for information security.

Appendix A Definitions

Term	Definition
Accreditation Boundary	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term <i>security perimeter</i> defined in the Committee on National Security Systems (CNSS) Inst 4009 and Director of Central Intelligence Directive (DCID) 6/3
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in accordance with defined procedures, whether automated or manual. [OMB Circular A-130, Appendix III] (Also referred to as IT System)
Information Technology (IT)	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)
Internet Protocol (IP) Network	For the purposes of this policy, any collection of devices communicating over a wired or wireless network using the Internet Protocol (IP)
NASA Guest Network	A NASA owned and managed accredited network on NASA IP space with a defined accreditation boundary that allows individual workstations at the NASA Headquarters or Centers to connect with the public intranet but has no connection to other NASA systems or networks that use NASA IP space
NASA Information	Any knowledge that that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA. (NPR 2810.1.)
Network	Information System implemented with a collection of interconnected nodes. (CNSS Instruction 4009)
Non-Public	See "Private" NASA IT System
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

Term	Definition
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
"Private" NASA IT System	Those NASA IT systems to which access is restricted and appropriately controlled through a formal process. Granting of access is contingent upon a favorable security background investigation commensurate with the risk level of the system
"Public" NASA IT System	Those NASA IT systems to which access is unrestricted
System	The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose.

Appendix B Acronyms

CIO	Chief Information Officer
CNSS	Committee for National System Security
DCID	Director of Central Intelligence Directives
FIPS	Federal Information Processing Standards
IP	Internet Protocol
ISO	Information System Owner
IT	Information Technology
ITSM	Information Technology Security Manager
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
PDA	Personal Digital Assistant
POA&M	Plan of Action and Milestones
SAISO	Senior Agency Information Security Officer
SSP	System Security Plan

Appendix C Information Technology (IT) Waiver Process.

Waivers to Information Technology (IT) Policies, Procedures, Standards, or Federal Requirements

1. Waivers to IT policies, procedures, standards or requirements standards, shall be granted by the NASA CIO.
2. The NASA CIO may delegate authority and responsibility to Center CIOs for a specific type of IT waiver or for a specific program or issue.
 - 2.1. The NASA CIO delegation of waiver authority and responsibility shall be in writing for the specific delegated authority or be as specified in NASA policy directives, e.g. in an NPR.
3. The individual/office preparing the waiver request shall submit the waiver request to the cognizant Center CIO for Center CIO concurrence and action. Example: The Sounding Rocket Program at the Wallops Flight Facility would submit the waiver to the GFSC CIO for review and concurrence/non-concurrence.
4. The waiver request shall include:
 - a. The NASA IT policy, procedure, standard, and/or Federal requirement to be waived.
 - b. The reason and justification for the waiver is required including:
 - (1) Risk Assessment;
 - (2) Cost-Benefit Analysis;
 - (3) Business Impact Assessment;
 - (4) Identification of compensating controls/actions;
 - (5) Proposed period of time for the waiver;
 - (6) The proposed date by which the Center will be compliant with the NASA IT standard, security control, and/or Federal requirement; and
 - (7) For an IT security control waiver or for any waiver that results in an unmitigated security weakness or deficiency, an Authorization Official (AO) approved Program of Action and Milestone (POA&M) shall be included with the waiver request.
5. The Center CIO shall evaluate the waiver and either concur or non-concur within 30 calendar days of receipt.
 - a. Non-concurred waivers shall be returned to the requester.

- b. Non-concurred waivers may be escalated to the Center Director or designee.
- 6. The Center CIO will forward the waivers with concurrence to the NASA CIO.
- 7. The NASA CIO shall evaluate the waiver request and the Center concurrence and either approve or disapprove the request within 30 calendar days of receipt.
- 8. For waivers to requirements contained in NASA policy documents, this waiver process applies only to those policy documents for which the Office of the CIO is responsible. For waivers to requirements in NASA policy documents for which the NASA CIO is not responsible, the requester shall follow the waiver process called out in the NASA policy document itself.