

# **NASA Information Technology Requirement**

**NITR-2830-1C**

**Effective Date: February 12, 2009**

**Expiration Date: [Month] {Day}, [Year]**

---

**Networks Using NASA Internet Protocol (IP) Resources 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 Using NASA IP Resources or NASA Physical Space**

- 1.1 Requirement
- 1.2 Responsibilities
- 1.3 Waivers

### **Appendix A Definitions**

### **Appendix B Acronyms**

### **Appendix C Information Technology (IT) Waiver Process.**

### **Distribution**

**NODIS**

**Center Chief Information Officers**

## Change History

Change Number	Date	Change Description
Change 1 by NITR-2830-1A	03/12/2009	Revised paragraph 1.1.1b for clarification of a non-NASA network or system.
Change 2 by NITR-2830-1B	02/17/2011	Updated expiration date to align it with NPR 2830.1, NASA Enterprise Architecture. Expiration date is now August 9, 2011.
Change 3 by NITR-2830-1C DRAFT	03/13/2011	Added additional IP address management, domain name service (DNS), and dynamic host configuration protocol (DHCP) requirements.
NITR-2830-1C PRELIMINARY	04/02/2012	Changed Section 1.1.1 wording to orient document to infrastructure vs. end devices; Deleted Appendix C - Waivers and changed Section 1.3 Waivers to reference NITR-2800-1.
NITR-2830-1C PRELIMINARY v2	04/11/2012	Backed out Section 1.1.1 wording to better allow for telework devices and bring-your-own-device without constraining need for use of IPAM for end devices.
NITR-2830-1C PRELIMINARY v3	04/11/2012	Changes resulting from Comm. Services Board contingent approval.
<a href="#">NITR-2830-1C PRELIMINARY v4</a>	<a href="#">10/30/2012</a>	<a href="#">Updated for name change of IPAM service to DDI service</a>

## **PREFACE**

### **P.1 PURPOSE**

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

### **P.2 APPLICABILITY**

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 resources 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**

None

### **P.6 CANCELLATION**

The next version of NPR 2830.1 cancels this NITR.

---

Linda Y. Cureton  
Chief Information Officer

---

Date

---

## 1.0 Requirements for Networks Using NASA IP Resources or NASA Physical Space

---

### 1.1 Requirement

#### 1.1.1 Internet Protocol (IP) Address Management

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

- a. Internet Protocol (IP) resources that have 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 for use on any non-NASA systems or networks is prohibited.
  - i. Personal and other non-NASA devices used for telework and bring-your-own-devices (BYOD) are not addressed in this policy. Use of these devices are expected to be governed by separate policies related to end-device network access admission and control.
  - ii. End-user devices or personal devices used to telework or access NASA networks must adhere to applicable NASA and federal policies and requirements.
- b. The construction and establishment of any non-NASA system or network, or use of non-NASA IP resources within the NASA accreditation boundary is prohibited.
- c. All address space shall be registered and maintained in the Agency [DDI \(DNS, DHCP, and IP address management \(IPAM\)\)](#) system, including private or non-routeable address space, whether configured in the domain name system (DNS) or not.
- d. All Autonomous System Numbers (ASN) shall be registered in the Agency [IPAMDDI](#) system.
- e. NASA address space shall be allocated by authorized personnel only.
- f. Non-NASA IP address space that is utilized within the NASA environment shall be registered in the Agency [IPAMDDI](#) system. This address space must have an approved waiver.
- g. NASA IP addresses shall be used only with authorized domains registered to NASA by the Agency OCIO Communications Service Office (\*.nasa.gov only, except by approved written waiver).

#### 1.1.2 Domain Name Service (DNS)

- a. All DNS services must be operated within the Agency [IPAMDDI](#) system. A waiver may be granted for the underscore domains for NASA Consolidated Active Directory to be managed on local domain controllers.
- b. NASA domain names shall be advertised only for NASA IP address space.

- c. DNS zone transfers are not permitted to ~~non-IPAM~~ DNS servers external to the Agency DDI system.
- d. Zone forwarding from local IPAMDDI DNS servers to ~~non-NASA DNS~~ servers external to the Agency DDI system is not permitted.
- e. All devices registered in DNS with an A (IPv4) and/or AAAA (IPv6) record must have a corresponding PTR record. Multiple PTR records for the same IP address is prohibited.
- f. Only the Agency IPAMDDI caching DNS servers may query the Internet directly.
- g. NASA DNS servers shall not be authoritative for non-NASA DNS domains except for domains managed within the Agency IPAMDDI system (e.g., nasa.org).
- h. DNS shall not be used as a security mechanism for applications (e.g., performing reverse lookups to allow access) unless/until the entire Agency is positioned to support such a configuration.
- i. Use of Dynamic DNS is encouraged and should be utilized where dynamic addressing methods are used, as appropriate. Guest DHCP is an example where Dynamic DNS would not be appropriate because these clients would not typically be registered in DNS.

### 1.1.3 Dynamic Host Configuration Protocol (DHCP)

- a. All DHCP must be operated under the Agency IPAMDDI system.
- b. Dynamic assignments are preferred over static or manual assignments, particularly in client networks, but increasingly for cloud/virtualized server environments. Static assignments will be allowed as appropriate.

## 1.2 Responsibilities

### 1.2.1 Center CIOs shall:

- a. Be responsible for ensuring compliance with this NITR or for ensuring that all non-compliant networks are operating under an approved waiver.
- b. Process 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 NITR-2800-1, NASA Information Technology Waiver Requirements and Procedures.

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
<a href="#">Agency DDI System</a>	<a href="#">The DNS, DHCP, and IPAM system operated by the NASA Office of the Chief Information Officer (OCIO) Communications Service Office (CSO).</a>
Information System (Also referred to as IT 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]
Dynamic Host Configuration Protocol (DHCP)	protocol used to assign addresses to clients from a pool of addresses; can also be used to distribute other configuration information. There are variants of DHCP deployments, to include both manual and dynamic methods.
Domain Name Service (DNS)	the automated means of converting human-readable system names into machine-readable Internet Protocol (IP) addresses
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)
IP Resources	For the purposes of this policy, NASA IP resources include IP addresses, Autonomous System Numbers, and domain names registered to NASA with regional Internet registries and domain registrars, as well as the servers that extend these IP resources in the form of DNS and DHCP services.
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

<b>Term</b>	<b>Definition</b>
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
"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 servers and resources that provide services to general Internet Users
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
<a href="#">DDI</a>	<a href="#">DNS, DHCP, and IPAM</a>
<a href="#">DHCP</a>	<a href="#">Dynamic Host Configuration Protocol</a>
<a href="#">DNS</a>	<a href="#">Domain Name Service</a>
<a href="#">DDNS</a>	<a href="#">Dynamic DNS</a>
FIPS	Federal Information Processing Standards
IP	Internet Protocol
<a href="#">IPAM</a>	<a href="#">IP address management</a>
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