National Aeronautics and
Space Administration

**RELEASE DATE**: 2020-06-12

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

**Prepared by:**

NASA Cybersecurity Standards and Engineering Team (CSET)

**Approved by:**

Michael Witt Digitally signed by Michael Witt
Date: 2020.06.23 07:18:46 -04'00'

Michael Witt
Senior Agency Information Security Officer

# Table of Contents

# Change History

| Change Number | Date | Change Description |
| --- | --- | --- |
| 1.0 | June 12, 2020 | Initial release created based on NITR 2830.1A |
| | | |
| | | |

## Purpose

The purpose of this NASA Advisory Implementing Instruction (NAII) is to establish policy and requirements regarding networks residing on or within NASA physical space and/or Internet Protocol (IP) space.

This NAII replaces NASA Information Technology Requirement (NITR) 2830.1A, *Networks in NASA Internet Protocol (IP) Space or NASA Physical Space*, which had an effective date of February 12, 2009, and was scheduled to expire on February 9, 2011.

## Applicability

This NAII is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This NAII applies to the NASA Jet Propulsion Laboratory, a Federally Funded Research and Development Center, and other contractors only to the extent specified or referenced in applicable contracts.

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 purposes of this document:

- IP addresses include both IPv4 and IPv6 as well as their defined multicast addresses.
- Systems are defined by their hardware and software component inventories and an authorization boundary as canonically defined within the Risk Information Security Compliance System (RISCS), which is the current Agency system of record.
- The scope of NASA IP space includes all addresses allocated and registered to NASA by ARIN or similar registries.

This NAII does not apply to personal devices such as cell phones 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.

## Authority

Per NASA Policy Directive (NPD) 2800.1, *Managing Information Technology*, 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/or 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.

## Applicable Documents

a. NASA Policy Directive (NPD) 2800.1, *Managing Information Technology*.

b. NASA Procedural Requirements (NPR) 2810.1, *Security of Information Technology*.

c. NPD 2540.1, *Acceptable Use of Government Office Equipment Including Information Technology*.

## Measurement and Verification

None.

## Cancellation

This NAII cancels NITR 2830.1A, *Requirements for Networks in NASA IP Space or NASA Physical Space*.

## Requirements

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

1. All NASA IP addresses shall be registered and managed within the NASA DNS, DHCP, and IPAM (DDI) System.
    a. The NASA DDI System is the authoritative repository for all NASA IP Addresses
2. Internet Protocol (IP) address space that has been registered, allocated, and assigned to NASA shall only be used to service NASA systems or systems authorized by NASA to support specific NASA Programs and/or Projects. 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.
3. The construction, establishment, or operation of any non-NASA system or network within the NASA authorization boundary and/or on GFE is prohibited.

    A non-NASA system or network is any system or network that does not possess a NASA authorization to operate and/or is not used in support of a NASA Program or Project.

    The only exception is for the use of individual workstations on the NASA Headquarters and Center Visitor, Partner and other special purpose Networks. In such a situation, the Visitor, Partner and other special purpose Networks shall (1) have a defined accreditation boundary, (2) be accredited with an authority to operate, and (3) have no connection between the Guest Network and other NASA systems or networks that use NASA IP address space.
4. Any deviation for this NAII shall be authorized as a risk-based decision (RBD) per NPR 2810.1*x*, *Security of Information Technology*.

# Appendix A: Acronyms

| | |
| --- | --- |
| CIO | Chief Information Officer |
| DDI | DNS, DHCP, IPAM |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Service |
| GFE | Government-furnished Equipment |
| IP | Internet Protocol |
| IPAM | Internet Protocol Address Management |
| IT | Information Technology |
| NAII | NASA Advisory Implementing Instruction |
| NASA | National Aeronautics and Space Administration |
| NITR | NASA Information Technology Requirement |
| NPD | NASA Policy Directive |
| NPR | NASA Procedural Requirements |