



**U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION**

**ORDER
JO 1370.117**

Air Traffic Organization Policy

Effective Date:
01/21/2014

SUBJ: National Airspace System (NAS) Internet Protocol (IP) Addressing Policy

1. Purpose of This Order. The purpose of this order is to formalize the management and assignment of National Airspace System (NAS) Internet Protocol (IP) Addresses for all device connections within the protected domain of the NAS. This order:

a. Defines the requirements and processes for NAS Systems Owners to acquire and use approved IP addresses from the Federal Aviation Administration's (FAA) IP address pool within the NAS Domain, as issued by the Communications, Information, and Network Programs (CINP) Group (AJM-31);

b. Addresses the assignment of NAS device IP addresses required for inter-facility and intra-facility communication between NAS devices;

c. Addresses the assignment of NAS device IP addresses needed by NAS sponsoring programs and/or users requiring IP service connectivity outside of the NAS Domain, such as a non-NAS system/network connected via one of the approved NAS Enterprise Security Gateways (NESGs); and

d. Facilitates the smooth operation, management, and administration of IP addresses and the recovery of defunct address spaces from the current assignments.

2. Audience. This order is intended for all NAS Sponsoring Programs and NAS users. It addresses all IP-addressable devices, products, and services within the NAS Domain of the FAA, NAS data and associated flows, and access to/from the NESG for both NAS and non-NAS data transfer to non-NAS users.

3. Where Can I Find This Order? You can find an electronic copy of this order on the Directives Management System (DMS) website: https://employees.faa.gov/tools_resources/orders_notices/. Or go to the MyFAA Employee website, select 'Tools and Resources', then select 'Orders and Notices'.

4. Scope. This order applies to all NAS systems, NAS inter/intra-facility telecommunications, the supporting Wide Area Network (WAN) infrastructure, and all interfaces from the NAS Domain to non-NAS systems/networks.

5. Policy.

a. NAS Device Intra-Facility, Inter-facility Telecommunications and WAN IP Communications within the NAS Domain.

(1) Information System Owners (ISO) must use approved NAS IP addresses from the FAA pool as assigned by the CINP Group (includes public, private, and multicast IP addresses). This applies to all system devices that exist within the NAS Domain and communicate via IP over any Local Area Network or WAN that are not physically isolated from all NAS shared IP Networking services [e.g., Telecommunications Infrastructure (FTI) Operational IP (OPIP) Network or NESG Demilitarized Zones (DMZ) environment]. Each NAS system device must use a unique NAS IP address from the assigned subnet(s) at the device location.

(2) ISOs for all existing NAS systems that contain devices that exist within the NAS Domain and currently use IP addresses that do not conform to this order, must migrate their system(s) to the approved IP addresses from the FAA pool as assigned by the CINP Group within one (1) year of the signature date on this order. NAS systems that do not comply with this order will have a Plan of Action and Milestones (POA&M) generated as part of their System Authorization package.

b. NAS Device IP Connectivity to Non-NAS Networks and Non-NAS Systems.

(1) For NAS Domain devices with IP connections to non-NAS Networks or non-NAS systems, ISOs must utilize approved internal and external NAS IP addresses from the FAA pool as assigned by the CINP Group (includes public, private, and multicast IP addresses).

(2) For NAS Domain devices with IP connections to non-NAS Networks or non-NAS Systems that do not conform to 5.b.(1), ISOs must migrate their device(s) to approved internal and external NAS IP addresses from the FAA pool as assigned by the CINP Group within one (1) year of the signature date on this order. ISOs must document via a POA&M how they will migrate their system to comply with this order. Systems that are not able to comply with this order within one (1) year must have an Authorizing Official Designated Representative (AODR)-approved migration plan within one year of the signature date on this order.

c. NAS Systems with Devices Outside of the NAS Domain.

(1) ISOs for all NAS systems with devices that reside outside of the NAS Domain, such as the Mission Support Domain, must clearly identify those devices in the System Characterization Document (SCD) of the System Authorization/Annual Assessment Package. The SCD must include, at a minimum, the following information for each device:

- (a) Device Locations(s);
- (b) IP Address (if Static) or Subnet Dynamic Host Configuration Protocol at each location; and
- (c) Statement indicating which FAA organization manages their IP addresses.

d. IP Address Management Via a Centralized Enterprise NAS IP Address Management/Tracking System.

(1) NAS ISOs must perform an analysis of the current NAS IP address allocations as a baseline, and coordinate the baseline with the CINP group at 9-AJW-NAS-IPAddressRequest@FAA.GOV.

(2) NAS ISOs needing IP addresses assigned must contact the CINP Group at 9-AJW-NAS-IPAddressRequest@FAA.GOV.

(3) NAS ISOs who no longer need IP addresses must contact the CINP Group at 9-AJW-NAS-IPAddressRequest@FAA.GOV so that the addresses can be placed back in the free pool of addresses.

(4) The CINP Group reserves the right to inventory/audit and continuously monitor the use of IP addresses via the OPIP network. NAS Information System Owners are required to allow these audits.

(5) The CINP Group reserves the right to reclaim unused NAS IP addresses in coordination with ISOs.

e. General NAS IP Addressing.

(1) The only public IP addresses permitted within the NAS Domain are from the FAA pool specifically assigned by the CINP Group.

(2) Use of Internet Engineering Task Force (IETF) reserved IP address ranges as specified in Requests For Comment (RFC) is not permitted. This order does not preclude use of special use IP addresses as defined in IETF RFC 5735.

(3) Use of Network Address Translation, Port Address Translation, and Port Forwarding by any programs in the NAS other than the FTI program, is not permitted without approval of the NAS AODR.

(4) Use of embedded IP Addresses in any NAS system software that prohibits migration of the system to NAS managed IP Addresses is not permitted.

6. Roles and Responsibilities. The following delineates roles and responsibilities for implementation of this policy.

a. NAS Authorizing Official (AO), AJW-0:

- (1) Is the custodian for the IP Addressing Policy;
- (2) Makes all determinations to terminate NAS inter/intra-facility and NESG connections for failure to comply with this order; and
- (3) Delegates authority to the NAS AODR for waiver exceptions.

b. NAS AODR, AJW-0:

- (1) Makes recommendations to the AO to terminate NESG and inter/intra-facility connections that fail to comply with this order;
- (2) Performs periodic compliance checks to ensure adherence to this order;
- (3) Reviews processes and procedures required to implement this order; and
- (4) Reports to the AO on risk mitigation plans and new vulnerabilities that would necessitate updates to this order.

c. NAS ISO:

- (1) Ensures compliance with the requirements stated in this order;
- (2) Directs any IP addressing and architectural questions or issues associated with FAA compliance to the AODR;
- (3) In coordination with the Information Systems Security (ISS) Group (AJW-B4), generates and schedules POA&Ms to bring systems into compliance with this policy;
- (4) Performs an analysis of the current NAS IP address allocations as a baseline, and provides the baseline to the CINP group;
- (5) Reports NAS IP address changes to the CINP group; and
- (6) Coordinates with the CINP Group to return unused IP addresses.

d. CINP Group:

- (1) Is the custodian of the metadata of NAS IP addresses;
- (2) Administers NAS-compliant IP addresses upon request to FAA programs; and
- (3) Defines and implements an IP Address Management Platform to maintain an accurate IP address baseline.

e. ISS Group (AJW-B4): In accordance with NAS ISOs, generates and schedules POA&Ms to bring systems into compliance with this policy.

7. Notice of Exception or Non-Compliance.

a. This order establishes policy to comply with statutory and regulatory requirements, including National Institute of Standards and Technology information systems security publications made mandatory by the Federal Information Security Management Act of 2002.

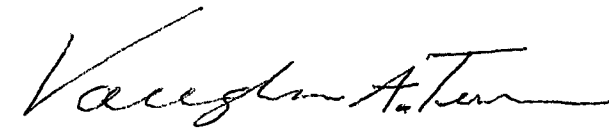
b. Penalties for user noncompliance with this order may include suspension of system privileges.

c. The ISO can request that the AODR grant relief from compliance. The following guidance is provided for requesting relief from this policy:

(1) All requests for relief must be submitted via email to the NAS AODR using the Subject Heading; "NAS IP Addressing Relief Approval Request for <System Name>". The email must define the specific policy statement(s) for which relief is being requested, justification for the relief, and any compensating controls that support a relief decision;

(2) The CINP Group must be copied (CC) on the request at 9-AJW-NAS-IPAddressRequest@faa.gov; and

(3) System Devices that are provided relief may be designated by the AO and/or AODR as external to the NAS and be migrated to using one of the approved NESGs.

A handwritten signature in black ink, appearing to read "Vaughn A. Turner". The signature is fluid and cursive, with a long horizontal stroke at the end.

Vaughn A. Turner
Vice President, Technical Operations Services

Appendix A. Administrative Information

1. Distribution. This order is distributed to all ATO field facilities with a standard distribution.

2. Definitions. Definitions of specialized terms used in this subject area, with relevant abbreviations and acronyms.

a. National Airspace System (NAS): The personnel, airspace, aircraft, equipment, and any and all other aviation components that comprise the United States' Aviation System.

b. NAS Domain: The Operational environment of the FAA that is under the controlling authority of the ATO, Technical Operations Directorate, which has responsibility for security measures related to IP data flows. The NAS Domain is defined in FAA Order 1370.116, Boundary Protection Policy, as "a separate security perimeter within the FAA Enterprise that provides an environment for NAS programs to operate and share information to support Air Traffic control operations." The NAS Domain includes the NESG and the NESG Internal and External DMZ which are used to communicate with non-NAS systems and/or networks. All other domains, such as the Administrative (Mission Support) and Research & Development Networks are considered non-NAS Domains. A notional NAS IP Address Boundary/ Control diagram is provided in Appendix B.

c. NAS System: A system that operates in the NAS environment and has been designated as 'NAS' in the ATO ISS Program Authorization Inventory (based on performance of NAS functions as defined in the NAS-RD-2010 and/or direct connectivity with the NAS Operational networking/computing environment).

d. NAS User(s): Any organization or person that operates or manages airspace operations within the NAS utilizing NAS resources.

e. Non-NAS User(s): Any organization or person that utilizes NAS resources from outside the NAS Domain and is not engaged in the operations or management of the NAS airspace.

f. NAS Data: Real time operational data used by the FAA to manage the flow of aircraft within the NAS.

Note: Near-real time NAS Data (delayed) is used in Situational Awareness systems by non-NAS users that are not engaged in the operations or management of the NAS airspace.

g. NAS NESG: The NESG provides a framework for complying with boundary protection service requirements between NAS and non-NAS systems/networks in accordance with ATO Order 1370.114, Implementation of Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Services and Information Security Requirements in the National Airspace System (NAS). The NESG infrastructure includes a layered security scheme to facilitate defense in depth security controls and provides a buffer between the NAS and external systems/networks.

h. NAS Sponsoring Program(s) / Information System Owner: Any Program Office of a NAS system as defined in the Information Systems Security Inventory.

i. Non-NAS Data: Any data that is generated outside of the NAS that is not managed through the NAS Configuration Change Board and may or may not have an Interface Requirement Document (IRD) or Interface Control Document (ICD). If an ICD or IRD exists, it describes the data and interface of the Non-NAS data at the NAS Enterprise Security Gateway and is governed by the NAS External Boundary Protection Service per FAA Order 1370.116, effective April 16, 2012, or as amended. Non-NAS data is generated outside of the FAA System Authorization boundary.

j. Private IP Address: Private IP Addresses are defined in IETF RFC 1918.

3. References.

- a.** FAA Order 1200.22, External Requests for NAS Data, as amended
- b.** FAA Order 1370.82A, Information Systems Security Program, as amended
- c.** FAA Order JO 1370.98, ATO Information Technology (IT) Infrastructure Requirements for Non-FAA Connectivity, as amended
- d.** FAA Order JO 1370.101, ATO Information Security Incident Reporting and Response Policy, as amended
- e.** FAA Order JO 1370.114, Implementation of Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Services and Information Security Requirements in the National Airspace System (NAS), as amended
- f.** FAA Order 1370.115, Domain Name System (DNS) Security Policy, as amended
- g.** FAA Order 1370.116, Boundary Protection Policy, as amended
- h.** FAA Order 1375.1, Information/Data Management, as amended
- i.** FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI), as amended
- j.** FAA Order 1800.66, Configuration Management Policy, as amended
- k.** OMB Circular Number A-130, Management of Federal Information Resources, November 28, 2000.
- l.** OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006.

- m.** IETF RFC 1918, Address Allocation for Private Internets, as amended
- n.** IETF RFC 3171, IANA IPv4 Multicast Guidelines, as amended

Appendix B. NAS IP Address Boundary/Control Diagram