DoD Instruction 8440.02

DoD Implementation of Internet Protocol version 6

Originating Component:	Office of the DoD Chief Information Officer
Effective:	December 17, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Directive-type Memorandum 21-004, "Department of Defense Implementation of Internet Protocol Version 6," June 29, 2021
Approved by:	Leslie A. Beavers, Acting DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive 5144.02, this issuance establishes policy, assigns responsibilities, and prescribes procedures for deploying and using Internet Protocol version 6 (IPv6) in DoD information systems.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSD, the Military Departments (including the United States Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. This issuance does not apply to systems that Section 3552(b)(6) of Title 44, United States Code defines as national security systems (NSS). However, NSS are not precluded from implementing IPv6 of their own accord.

1.2. POLICY.

All new networked DoD information systems, used by DoD Components, which use internet protocol technologies, will be IPv6-enabled before their implementation and operational use, pursuant to the guidance contained in the DoD IPv6 Implementation Plan in Paragraph 3.2 of this issuance.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

The DoD CIO:

a. Establishes policy and provides guidance to implement the operational deployment of IPv6 in coordination with the:

(1) Director, Defense Information Systems Agency (DISA).

(2) Director, National Security Agency/Chief, Central Security Service.

(3) CJCS.

(4) Commander, United States Cyber Command.

(5) Other DoD Component heads.

b. Directs and oversees new networked DoD information systems to require that they are IPv6-enabled before their implementation, pursuant to the timelines contained within the DoD IPv6 Implementation Plan.

c. Monitors the DoD's IPv6 implementation status and the replacement or retirement of information systems and applications that are not IPv6-capable to oversee progress toward IPv6-only deployment.

d. Reviews all requests to waive stated IPv6 requirements on a case-by-case basis to determine whether implementing these IPv6 capabilities would pose a risk of failure or a prohibitive cost for an acquisition. See Paragraph 3.3. for further details for the waiver process.

e. Requires systems that support enterprise security services are IPv6-capable and operable in IPv6-only environments.

f. Certifies all elements of the Department of Defense information network (DoDIN) and DoD Component-operated network information technology security plans, architectures, and acquisitions, to include IPv6 objectives and plans for fully implementing IPv6.

g. Monitors and evaluates IPv6-only pilots and dual stack (Internet Protocol version 4 (IPv4) and IPv6), hereafter referred to in this issuance as dual stack, limited deployment expansions that are transitioning to operational systems, and reports progress quarterly to the Office of Management and Budget.

h. Coordinates IPv6 interfaces with the Federal IPv6 Task Force, which oversees the Federal Government's adoption and implementation of IPv6.

i. Provides and maintains a current electronic means for DoD Components to submit, manage, and deconflict IPv6 priorities, plans, and requirements.

j. Maintains the DoD IPv6 Implementation Plan.

2.2. DIRECTOR, DISA.

Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.4., the Director, DISA:

a. Executes IPv6 responsibilities and functions in accordance with U.S. Government and Office of Management and Budget policy and direction and this issuance.

b. Maintains an IPv6 program management office to help manage and deconflict IPv6 priorities and plans.

c. Reviews, in coordination with the DoD CIO, the process of standardizing dual stack and IPv6-only connectivity to all DoD Components, as a standard Defense Information Systems Network (DISN) service (i.e., without specifically requesting IPv6 service in DISA Storefront, or in the ServiceNow portal) for all existing IP-enabled customer interfaces every six months.

d. Establishes and maintains a knowledge base for the DoD community in a SharePoint or web portal format that provides:

(1) IPv6 lessons learned from various IPv6 pilot testing and limited deployments.

(2) IPv6 training resources for network engineers and cybersecurity personnel.

(3) IPv6 lessons learned for network managers and operators.

e. Updates and maintains IPv6 standards and implementation profiles in the DoD Information Technology Standards Registry, available at https://gtg.csd.disa.mil/disr/dashboard.html, in coordination with the National Institute of Standards and Technology (NIST) IPv6 U.S. Government version 6 (USGv6) Test Program.

f. Operates a DoD Network Information Center (NIC) that acquires and manages all respective IPv6 addressing resources and updates and maintains the DoD IPv6 Address Plan.

g. Develops and updates test processes to assess compliance with the IPv6 requirements for the DoDIN Approved Products List and, when appropriate, leverages the NIST USGv6 Test Program for basic IPv6 conformance and interoperability testing of commercial products.

h. Enables developmental, operational, interoperability, and cybersecurity testing of IPv6-enabled information technology in coordination with the Joint Interoperability Test Command.

i. Provides IPv6-enabled access to commercial cloud services required by the timelines provided in the DoD IPv6 Implementation Plan.

j. Provides dual stack and IPv6-only DISA ecosystem service to its customers by the timelines provided in the DoD IPv6 Implementation Plan.

k. Updates and maintains the Security Technical Implementation Guides and Security Requirements Guides on the DoD Cyber Exchange Website, which requires that new and existing guides contain appropriate IPv6 cybersecurity requirements.

2.3. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

In addition to the responsibilities in Paragraph 2.4., under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security, and the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information Systems Security Program:

a. Verifies that internet access point systems provide equivalent IPv4 and IPv6 capabilities.

b. Provides cybersecurity guidance on an as-needed basis to support DoD IPv6 deployments.

c. Provides technical input for updating and maintaining IPv6 standards registries.

d. Identifies, assesses, and develops IPv6 training from appropriate requirements.

e. Provides reporting of IPv4 and IPv6 attack sensing and warning and cyber threat intelligence.

2.4. DOD COMPONENT HEADS AND COMMANDANT, UNITED STATES COAST GUARD.

The DoD Component heads and the Commandant, United States Coast Guard:

a. Direct that new networked DoD information systems that utilize internet protocol technologies are IPv6-enabled before implementation and operational use.

b. Verify that commercially hosted public-facing unrestricted services are IPv6-enabled.

c. Develop and execute plans for converting, replacing, or retiring inventoried information systems and applications that are not IPv6-capable to enable transition to IPv6-only deployment.

d. Identify DoD Component-hosted, public-facing, unrestricted services and develop plans (e.g., retain in place, transition to cloud by date, and retire by date) for transition to IPv6-only deployment.

e. Identify objectives and plans for full IPv6 support in information technology security plans, architectures, and acquisitions to advance networked information systems, and the IP-enabled assets associated with these systems, to enable native IPv6 operations fully.

f. Requires that new products provide equivalent IPv4 and IPv6 capabilities and can function in IPv6-only mode.

g. Transition cybersecurity systems to provide equivalent IPv4 and IPv6 capabilities and develop action plans and milestones to resolve gaps in accordance with the DoD IPv6 Implementation Plan.

h. Monitor network performance and security operations to oversee secure IPv6 implementation.

i. Determine that applications and systems migrated to commercially hosted cloud services are IPv6-only capable, and if provider limitations exist, obtain a resolution roadmap.

j. Identify appropriate resources required to support actions directed in this issuance and incorporate them into future program objective memorandum submissions.

k. Establish policies and provide procedures to ensure relevant personnel are trained to execute IPv6 transition plans.

l. Identify opportunities and execute IPv6 pilots to enable migration to IPv6-only operations.

m. Perform the necessary ordering and provisioning actions to make all external connections dual stack, including:

(1) Performing the necessary validation to confirm IPv6 is enabled and working properly on all dual stack nodes.

(2) Coordinating with DISA Consolidated Provisioning and the Customer Advocacy and Service Activation groups for DISN connections.

2.5. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.4., the Commander, United States Cyber Command, establishes requirements for IPv6 training and tools for cyberspace operations forces personnel.

SECTION 3: PROCEDURAL IMPLEMENTATION GUIDANCE

3.1. GUIDELINES.

a. Networked environments, including the IP-enabled assets associated with them, will evolve to fully enable IPv6-only operations. Access to DoDIN applications or services, as well as access to native IPv6 internet content, will be accomplished via native IPv6 from within the DoDIN.

b. DoD public-facing unrestricted servers and services (e.g., sites and services that do not require authentication) will be accessible and functional using IPv6-enabled platforms and devices.

c. DoD contracts for the acquisition of networked information technology hardware, software, and services must include explicit requirements for IPv6 capabilities using the NIST USGv6 profile.

d. Compliance with the NIST USGv6 profile will be required and, where possible, the DoD will use the NIST USGv6 Test Program for basic conformance and interoperability testing of commercial products.

e. DoD systems that support enterprise security services will be dual stack enabled and capable of operating in IPv6-only environments pursuant to the timelines contained in the DoD IPv6 Implementation Plan. Examples of these DoD enterprise security service devices include, but are not limited to:

(1) Identity and access management systems.

(2) Firewalls.

(3) Intrusion detection and protection systems.

(4) End point security systems.

(5) Security incident and event management systems.

(6) Access control and policy enforcement systems.

(7) Threat intelligence and repudiation systems.

f. DoD's initial focus is to implement IPv6 in traditional information technology assets that primarily use internet protocol with the expectation that systems, such as non-NSS, the Nonclassified Internet Protocol Router Network, facility related control systems and/or industrial control systems, and any other operational technology systems, will also implement IPv6 when those systems and environments start utilizing traditional information technology products within their environments and they are IPv6-capable.

3.2. DOD IPV6 IMPLEMENTATION PLAN.

a. The DoD IPv6 Implementation Plan, a living document, describes the DoD transition process, including a life-cycle approach with milestones and actions for DoD Components to follow. This plan:

(1) Prescribes the phasing requirements for when IP-enabled assets on DoD networks must operate in IPv6-only environments, as required.

(2) Identifies and justifies DoD information systems that cannot be converted to use IPv6 and provides a schedule for replacing or retiring these systems.

b. The customer premise equipment must support IPv6. All existing and new IP-enabled customer edge interfaces, facing the DISN provider edge or the joint base customer edge router, must be configured with an IPv6 address.

(1) The DoD IPv6 Address Plan, currently Version 1.3, and all future versions, are the certified and authoritative address assignment plan for the end-nodes that communicate with the public internet.

(2) All tenants and customers at a base, post, camp, or station will be provided an IPv6 prefix by the DoD NIC in accordance with the latest approved plan.

(3) The DoD IPv6 Address Plan can be found at https://www.nic.mil, under "Policy Guidance and Documentation."

3.3. WAIVERS.

DoD Components may request a waiver from the IPv6 policies in this issuance when requiring demonstrated IPv6 capabilities would pose a risk of failure or add prohibitive costs to an acquisition.

a. Only the DoD CIO may approve requests for waivers of the policy to use IPv6. The DoD CIO may grant waivers to this policy only:

(1) When the cognizant DoD Component head has validated an urgent operational need to implement IPv6, or to standup an information technology system; or

(2) To accommodate introduction of new technology pilot programs coordinated with and recommended by the Director, DISA, and validated by the DoD Component concerned.

b. To obtain a waiver to this policy, DoD Components must send a system-specific request to the DoD CIO justifying why compliance is not possible, and why the system must be fielded before compliance. The request must:

(1) Be in the form of a memorandum addressed to the DoD IPv6 Lead for the DoD CIO.

(2) Identify the system, including a description of planned deployment milestones, duration, rationale for non-compliance, and risk of failure or operational disruption resulting from IPv6 adoption, and documentation of the risk of failure or prohibitive cost absent a waiver.

3.4. DOD IPV6 ADDRESS PLAN STANDARD.

a. The DoD IPv6 Address Plan, maintained and published by the DoD NIC, is the address plan for all DoD Components to use for their enterprise end-nodes, services, and devices at each base, camp, post, and installation that are connected to the Nonclassified Internet Protocol Router Network and that communicate with the public internet.

b. All DoD Components are encouraged to utilize site assignments from this plan, and any exceptions to this plan must be submitted to and approved by the DoD NIC.

c. DoD top-level IPv6 allocation from the American Registry for Internet Numbers is subdivided into various separate hierarchical sub-allocations, with their definitions and usability within the DoDIN. DoD Components must review material available at the DoD NIC registration website, available at https://www.nic.mil, before starting any IPv6 address planning effort.

d. Components that seek exceptions to the DoD IPv6 Address Plan may send their requests to the CIO and include the DoD NIC for situational awareness. The DoD IPv6 Lead will review and coordinate approval as necessary.

3.5. QUARTERLY REPORTING OF IPV6 ENABLED ASSETS IN THE DOD INFORMATION TECHNOLOGY PORTFOLIO REPOSITORY (DITPR).

The DITPR is the authoritative repository to track IPv6 progress across the DoDIN.

a. The DoD Components will designate a DITPR identifier for all programs and will maintain a current inventory account of IP-enabled assets for such DoD Component programs.

b. The DoD CIO will use the DITPR as the authoritative source of inventory data for each DoD Component program to track progress of IPv6-enabled assets.

c. DoD Component program managers who manage systems in the DITPR will consult and follow the registry documentation for quarterly reporting requirements of IP-enabled assets.

d. The DoD IPv6 Working Group Secretary will provide all training for the DoD Components for entering the required reporting in the DITPR. DoD Component program managers who manage systems in the DITPR will use this training to properly document systems in the DITPR.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CJCS	Chairman of the Joint Chiefs of Staff
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITPR	DoD Information Technology Portfolio Repository
DoD CIO	DoD Chief Information Officer
DoDIN	Department of Defense information network
IP	internet protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
NIC	network information center
NIST	National Institute of Standards and Technology
NSS	national security systems
USGv6	U.S. Government version 6

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
dual stack (IPv4 and IPv6)	A system or product that can process both IPv6 and IPv4 packets, receive from or forward IPv6 packets to other IPv6-only and dual stack systems, and receive from or forward IPv4 packets to other IPv4-only and dual stack systems.
enterprise security services	Identity and access management systems, firewalls, intrusion detection and protection systems, end-point security systems, security incident and event management systems, access control and policy enforcement systems, and threat intelligence and repudiation systems.
IP	The global numeric identifiers necessary to identify uniquely entities that communicate over the internet.
IPv4	IP addresses in use since 1983.

TERM	DEFINITION
IPv6	Most recent version of the internet protocol designed to replace IPv4.
IPv6-capable	Refers to a system or service that has correctly implemented a complete set of IPv6 capabilities. The NIST USGv6 profile describes detailed technical requirements for IPv6 capabilities for distinct product types.
IPv6-enabled	Refers to a system or service in which the use of IPv6 is "turned on" for production use.
IPv6-only	Refers to the state of an operational system or service when IPv4 protocol functions (addressing or packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-only environments.

REFERENCES

DoD Chief Information Officer, "DoD IPv6 Address Plan Version 1.3," updated December 2021

DoD Chief Information Officer, "DoD Strategy to Implement Internet Protocol version 6 (IPv6)," November 1, 2019

DoD Cyber Exchange Public Website, "Security Requirements Guides"[1]

DoD Cyber Exchange Public Website, "Security Technical Implementation Guides"[2]

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD IPv6 Implementation Plan for Office of Management and Budget (OMB) Fiscal Years (FY) 2021-2025 Requirements[3]

United States Code, Title 44, Section 3552(b)(6)

[1] https://public.cyber.mil/

[2] https://public.cyber.mil/

[3] DoD IPv6 Implementation Plan for OMB FY2021-2015: https://dod365.sharepoint-mil.us/:b:/r/teams/DODCIO-IPv6WorkingGroup/Shared Documents/General/07 - DoD Component IPv6 Deep Dives/2023 Component IPv6 Deep Dives/IPv6 Documents Supporting Component Implementation/DoD IPv6 Implementation Plan FY 2021-2025--Signed Final 30 Sep 2021.pdf?csf=1&web=1&e=8BHoTD