DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON DC 20301-1010

June 29, 2021

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum 21-004 – "Department of Defense Implementation of Internet Protocol Version 6"

References: See Attachment 1

Purpose. Pursuant to the Federal requirements in Office of Management and Budget (OMB) Memorandum M-21-07, this directive-type memorandum (DTM):

- Establishes policy, assigns responsibilities, and prescribes procedures for deploying and using Internet Protocol version 6 (IPv6) in DoD information systems.

- Is effective June 29, 2021; it will be converted to a new DoD instruction. This DTM will expire effective 12 months from the date issuance is published on the DoD Issuances Website, June 29, 2022.

Applicability. This DTM:

- Applies to OSD, the Military Departments (including the 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 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 DoD (referred to collectively in this issuance as the "DoD Components").

- Does not apply to National Security Systems, as defined by Committee on National Security Systems Instruction 4009.

Definitions. See Glossary.

Policy. Pursuant to OMB Memorandum M-21-07, all new networked DoD information systems that use internet protocol (IP) technologies will be IPv6-enabled before implementation and operational use by the end of fiscal year (FY) 2023.

Responsibilities. See Attachment 2.

Procedures. See Attachment 3.

Releasability. Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Attachments:
As stated.

ATTACHMENT 1

REFERENCES

Committee on National Security Systems Instruction 4009, Committee on National Security Systems Glossary, April 6, 2015

DoD Chief Information Officer, "Charter for the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM)," July 13, 2020

DoD Chief Information Officer, "Department of Defense Digital Modernization Strategy, 2019-2023", June 5, 2019

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

DoD Chief Information Officer, "DoD IPv6 Address Plan" Version 1.2, September 2017

National Institute of Standards and Technology Special Publication 500-267, "USGv6 Profile," November 24, 2020

National Institute of Standards and Technology Special Publication 500-267Ar1, "NIST IPv6 Profile," November 24, 2020

Office of Management and Budget Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," November 19, 2020

ATTACHMENT 2

RESPONSIBILITIES

1. DoD CHIEF INFORMATION OFFICER (DoD CIO). The DoD CIO:

a. Establishes policy and provides guidance to implement this DTM, in coordination with the Director, National Security Agency; Commander, United States Cyber Command; Director, Defense Information Systems Agency (DISA); the Chairman of the Joint Chiefs of Staff; and other DoD Component heads for the implementation and operational deployment of IPv6.

b. Directs and oversees new networked DoD information systems to ensure that they will be IPv6-enabled before implementation and operational use by the end of FY 2023.

c. Directs and oversees at least one IPv6-only operational system pilot by the end of FY 2021.

d. Develops a DoD IPv6 implementation plan by the end of FY 2021 and updates the DoD Digital Modernization Strategy, as appropriate, to evolve networked DoD systems and the IP-enabled assets associated with these systems, to enable native IPv6 operation fully.

e. Monitors the DoD's IPv6 implementation status and the replacement or retirement of information systems and applications that are not IPv6-capable to ensure progress toward IPv6-only deployment; resolves challenges identified by the Digital Modernization Infrastructure (DMI) Executive Committee (EXCOM) in accordance with its July 13, 2020 charter.

f. Approves requests to waive stated acquisition requirements on a case-by-case basis where requiring demonstrated IPv6 capabilities would pose an undue burden on an acquisition action.

g. Requires systems that support enterprise security services to be IPv6-capable and operable in IPv6-only environments.

h. Requires DoD Core and Component information technology security plans, architectures, and acquisitions include IPv6 objectives and plans for fully implementing IPv6.

i. Monitors and evaluates IPv6-only pilots that are transitioning to operational systems and reports progress to the Secretary of Defense and OMB.

j. Coordinates IPv6 interfaces with non-DoD partners.

k. Develops and provides guidance for DoD Component IPv6 implementation plan content by the end of FY 2021.

2. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 4, the Director, DISA:

a. Executes IPv6 responsibilities and functions in accordance with applicable Federal and OMB policy and this DTM.

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

c. Requires the Defense Information Systems Network (DISN) to provide dual stack Internet Protocol version 4 (IPv4)/IPv6 and IPv6-only connectivity to all DoD Components as a standard DISN service (i.e., without specifically requesting IPv6 service) by the end of FY 2021.

d. Completes an IPv6-only operational system pilot by the end of FY 2021.

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

f. 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.

g. Updates and maintains IPv6 standards and implementation profiles in the DoD Information Technology Standards Registry at https://www.dsp.dla.mil/Specs-Standards/List-of-DISR-documents/ in conjunction with the National Institute of Standards and Technology (NIST) IPv6 U.S. Government version 6 (USGv6) Program.

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

i. Provides domain name system services to DISN-based IPv6-only users and networks via Enterprise Recursive Service for the .mil generic top-level domain, and .mil proxy for all external public facing services.

j. Updates and maintains the DoD Information Network (DoDIN) Approved Products List, leveraging the NIST/USGv6 Test Program for basic conformance and interoperability testing of commercial products.

k. Develops test processes to assess compliance with the IPv6 requirements in the DoDIN Capability Requirements for the DoDIN Approved Products List.

l. In coordination with the Network/Communications and DoD Information Network Capabilities Division of the Joint Interoperability Test Command, enables developmental, operational, interoperability, and cybersecurity testing of IPv6-enabled information

technology.

m. Provides IPv6-enabled access to commercial cloud services by the end of FY 2021.

n. Provides dual stack IPv4/IPv6 and IPv6-only DISA Ecosystem service to its customers by the end of FY 2022.

o. Updates and maintains the Security Technical Implementation Guides and Security Requirements Guides on the DoD Cyber Exchange site, requiring that new and existing guides contain appropriate IPv6 cybersecurity requirements.

p. Develops the Joint Regional Security Stack (JRSS) IPv6 implementation plan by the end of FY 2021 to identify required actions with proposed schedule, costs, milestones, and critical dependencies to deliver reliable and secure dual stack IPv4/IPv6 and IPv6-only services for JRSS customers.

q. Provides dual stack IPv4/IPv6 JRSS service to its customers beginning in FY 2022 and supports IPv6-only service starting in FY 2023.

3. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE. Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security, in addition to the responsibilities in Paragraph 4 of this attachment, and in coordination with the Director, DISA, the Director, National Security Agency/Chief, Central Security Service:

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

b. Provides cybersecurity guidance to support DoD IPv6 deployments as needed.

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

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

e. Provides IPv4/IPv6 attack sensing and warning, and cyber threat intelligence as available.

4. DOD COMPONENT HEADS. The DoD Component heads:

a. Require new networked DoD information systems that utilize IP technologies to be IPv6-enabled before implementation and operational use by the end of FY 2023.

b. Require commercially hosted public facing unrestricted services to be IPv6-enabled.

c. Develop an IPv6 implementation plan by the end of FY 2022 in accordance with

applicable DoD CIO guidance to meet the remaining milestones and actions in OMB Memorandum M-21-07.

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

e. Identify DoD 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.

f. 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.

g. Require that new cybersecurity products provide equivalent IPv4/IPv6 capabilities.

h. Transition cybersecurity systems to provide equivalent IPv4/IPv6 capabilities and develop action plans and milestones to resolve gaps.

i. Monitor network performance and security operations to ensure secure IPv6 implementation.

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

k. Identify additional resources required to support actions directed in this DTM and incorporate them into the program objective memorandum for FY 2023 and future program objective memorandum submissions.

l. Establish policies and provide procedures to ensure appropriate personnel are trained to execute IPv6 transition plans.

m. Identify opportunities and execute IPv6 pilots to facilitate migration to IPv6-only operations; complete at least one IPv6-only operational system pilot by the end of FY 2022.

5. COMMANDER, UNITED STATES CYBER COMMAND. In addition to the responsibilities in Paragraph 4, the Commander, United States Cyber Command establishes requirements for IPv6 training and tools for Cyber Mission Force personnel.

ATTACHMENT 3

PROCEDURES

1. DMI EXCOM. In conjunction with the DoD CIO, the DMI EXCOM will govern and enforce IPv6 transition efforts at the DoD level and identify challenges to be resolved to ensure progress is sustained.

2. GUIDELINES.

a. IPv4 use will be phased out for all government/commercial off the shelf information systems by either converting to IPv6, replacement, or retirement in accordance with the DoD and Federal IPv6 requirements in OMB Memorandum M-21-07 and the DoD Strategy to Implement IPv6.

b. Networked environments, including the IP-enabled assets associated with them, will evolve to enable IPv6-only operations fully.

c. Access to DoDIN applications or services will be accomplished via native IPv6 from within the DoDIN, as well as access to native IPv6 Internet content from DoDIN workstations.

d. DoD public-facing unrestricted servers and services will be accessible and functional using IPv6-enabled platforms and devices.

e. Acquisitions of networked information technology hardware, software, and services will contain contract clauses with explicit requirements for IPv6 capabilities using the NIST/USGv6 Profile.

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

g. DoD Components may request a waiver from the DoD CIO when requiring demonstrated IPv6 capabilities would pose an undue burden on an acquisition.

h. Systems that support enterprise security services (i.e., identity and access management systems, firewalls and intrusion detection/protection systems, end-point security systems, security incident and event management systems, access control and policy enforcement systems, threat intelligence and repudiation systems) will be dual stack IPv4/IPv6-enabled and capable of operating in IPv6-only environments by the end of FY 2025.

3. DOD IPV6 IMPLEMENTATION PLAN. The DoD CIO's IPv6 implementation plan will describe DoD's transition process and include milestones and actions pursuant to OMB Memorandum M-21-07. The plan will:

a. Require that at least 20 percent of IP-enabled assets on DoD networks are operating in IPv6-only environments by the end of FY 2023.

b. Require that at least 50 percent of IP-enabled assets on DoD networks are operating in IPv6-only environments by the end of FY 2024.

c. Require that at least 80 percent of IP-enabled assets on DoD networks are operating in IPv6-only environments by the end of FY 2025.

d. Identify and justify DoD information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMI	digital modernization infrastructure
DoD CIO	DoD Chief Information Officer
DoDIN	DoD information network
DTM	directive-type memorandum
EXCOM	Executive committee
FY	fiscal year
IP	internet protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JRSS	Joint Regional Security Stack
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
USGv6	U.S. Government version 6

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
dual stack IPv6/IPv4	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.
IP	The global numeric identifiers necessary to identify uniquely entities that communicate over the Internet.
IPv4	IP addresses in use since 1983.
IPv6	Next-generation IP designed to replace IPv4.

TERM	DEFINITION
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, 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.