DoD IPv6 Context and Way Ahead

Col Keith Repik
Department of Defense
Office of the Chief Information Officer
13 Jun 2019
Context

No hype at this stage – quiet adoption and evolution

Core nations of global digital economy are here.
DoD Direction, Intent and Rationale

- DoD CIO memo signed 27 Feb 2019
- Initial direction and guidance:
  - Purpose: Reinvigorate preparations and planning
  - Focus: Long lead time actions and enabling capabilities
  - Key Priorities: cybersecurity, cloud, applications, mobility, mission partners
  - Goal: Secure and reliable IPv6 services in support of DoD missions
- Achieve meaningful and measurable progress over the next 2 years, and maintain sustainable course thereafter
- Reduce risk and enable opportunities
- Multi-year effort to operationalize IPv6
  - People, processes, and technology ... plus experience
- Provide agility and cybersecurity in support of global DoD operations and partnerships
DoD Direction, Intent and Rationale

Attachment 1

Direction and Guidance for IPv6 Implementation

The Department’s goal is to secure and reliable services in support of DoD missions. Initial drivers are cybersecurity, cloud, mobility and mission partner interfaces. Major FY14-23 objectives include preparing unclassified DOD services and support for Internet-based capabilities. Implementation will be accomplished in an orderly manner that ensures acceptable security and reliability. Initial directions and guidance for implementation is provided below:

(2) DoD CIO will

a. Lead development of a DoD IPv6 Strategy for DoD EXCOM endorsement and DOD CC humanization

b. Determine DoD cybersecurity architecture and posture impacts using the DoD Cybersecurity Analysis and Review (DCAR) process NLT Q4FY19

c. Integrate IPv6 considerations into the DoD Cyber Security Reference Architecture (CSRA) NLT Q4FY19

d. Integrate IPv6 considerations into the DoD, DOD and Component Enterprise Data Center Reference Architecture NLT Q4FY19

e. Determine US government collaboration and cybersecurity information sharing (e.g. best practices, product assessments and roadmaps) opportunities NLT Q4FY19

f. Establish supplemental guidance to the acquisition of IPv6-capable products and services. The IPv6-capable definition requires support for both IPv4/IPv6 (i.e. dual stack) and IPv6-only environments. IPv6 support must be required. IPv6-only capability (i.e. no IPv4 deprecation) is optional to maximize dual stack operations.

g. Propose Defense Federal Acquisition Regulation Supplement (DFARS) guidance for acquisition of IPv6-capable products NLT Q4FY19

(7) Defense Information Systems Agency will

a. Designate a DISA IPv6 lead and establish a formal program management office

b. Develop a DISA IPv6 Implementation Plan for FY14-23 within 90 days of this memo. Include required actions with a scheduled start, end and critical dependencies to deliver reliable IPv6 services within the DISN, and as support of Internet-based capabilities.

c. Provide an electronic means for DISA Components to submit, manage and de-conflict IPv6 planning, plans and requirements NLT Q4FY19

d. Provide on demand IPv6 configuration training and access commercial advanced training resources for network engineers and cybersecurity personnel NLT Q4FY19

e. Provide on demand IPv6 training resources for network engineers and cybersecurity personnel NLT Q4FY19

f. Define and maintain IPv6 standards and implementation profiles in the Defense Information Technology Standards Registry (DITSTR) NLT Q4FY19

g. Verify Internet Access Point (IAP) systems provide equivalent IPv6/IPv4 capabilities and resolve gaps. Provide POA&Rs for any unsecured gaps NLT Q4FY19

h. Verify the Secure Cloud Computing Architecture (SCCA) provides equivalent IPv6/IPv4 capabilities and resolve gaps. Provide POA&Rs for any unsecured gaps NLT Q4FY19

i. Verify DoD Private Key Infrastructure (PKI) provides essential IPv6 functionality (e.g. DoD voucher requests) for enabling IPv6 services and resolve gaps NLT Q4FY19

j. Develop test processes and methodologies to assess compliance with DoD-related IPv6 requirements for Approved Products List (APL) testing NLT Q4FY19

k. Verify existing STS/SECOPs are consistent with IPv6-related cybersecurity requirements by Q4FY19

1. Verify TechCloud 2.0 provides equivalent IPv6/IPv4 capabilities and resolve gaps. Provide POA&Rs for any unsecured gaps NLT Q4FY19

m. Provide IPv4/IPv6 enabled Cyber Security Services NLT Q4FY19

n. Provide Domain Name System services to IPv6-only internal networks for the near term top level domains NLT Q4FY19

(3) National Security Agency will

a. Assist NSA in verifying that IAP systems provide equivalent IPv6/IPv4 capabilities.

b. Provide cybersecurity support in support of DoD IPv4 deployments as needed

c. Provide technical input to update and maintain IPv6 standards, requirements and processes as needed.

d. Assist NSA with IPv6 training implementation, assessment and development

e. Provide IPv-6 Attack Signatures, and Cyber Threat Intelligence, NLT Q4FY19

(6) United States Cyber Command will

a. Establish requirements for IPv6 training and tools for Cyber Mission Force personnel NLT Q4FY19

(7) DoD Components and the United States Coast Guard will

a. IPv6-enable all commercially hosted public facing unclassified services NLT Q4FY19

b. Monthly reporting will be accomplished with instructions to follow

c. Identify DoD limited public facing Internet services NLT Q4FY19

d. Issue DoD limited public facing services guidance (e.g. network operations) to define by date, transition to IPv6 by date, etc.) and dependencies to enable IPv6

(8) Ensure all cybersecurity products provide equivalent IPv6/IPv4 capabilities

(9) Verify existing cybersecurity systems provide equivalent IPv6/IPv4 capabilities and resolve gaps. Provide POA&Rs for any unsecured gaps NLT Q4FY19

i. Ensure all applications and systems migrated to commercially hosted cloud services are IPv6-only capable. If providers fail to备注 (Reserved randomly

j. Monitor and report minimum platform IPv6 plan results on a semi-annual basis, or as needed. Monitor and report minimum platform IPv6 plan results on a semi-annual basis, or as needed. Use existing engagement forums where possible (e.g. CCBR)

k. Identify any additional resources required to support actions detailed in this guidance and incorporate into Program Objective Memorandum FY21 submissions.