NATIONAL MEDIATION BOARD
WASHINGTON, D.C. 20572

July 20, 2021

MEMORANDUM FOR ALL NATIONAL MEDIATION BOARD EMPLOYEES

From: **William Fumey**

Chief Information Officer

Subject: **Internet Protocol Version 6 (IPv6) Compliance Directive**

Background

On December 10, 2009, the FAR was updated to require that all new IT acquisitions using IP must be IPv6 compliant. IPv6 replaces Internet Protocol version 4 (IPv4), and it is the most recent version of IP that provides an identification and location system for computers on networks and routes traffic across the Internet. Federal agencies are required to ensure IPv6 compliance when procuring networked IT products. On September 28, 2010, the Office of Management and Budget (OMB) issued a memorandum detailing the federal government's commitment to the operational deployment and use of IPv6 and provided guidance to ensure agency procurements comply with FAR requirements.

Some vendors have not implemented IPv6 with the same functionality as IPv4. To address this issue, the National Institute of Standards and Technology (NIST) developed the U.S. Government v6 Profile (USGv6) and defined it in the NIST Special Publication (SP) 500-267.

NIST SP 500-267 groups IT equipment into three categories: hosts, routers and network protection devices. Hosts include devices such as personal computers, printers, scanners or other end-point devices. Routers are devices such as switches, network routers, Wide Area Network accelerators, load balancers and other infrastructure-related equipment that transport IP traffic. Pure layer 2 switches are excluded as routers. Network protection devices help enforce IP security policy and include firewalls, intrusion detection/prevention systems, proxies and sniffers.

NIST SP 500-267 recommends the use of an IPv6 profile document to specify the IPv6 requirements to a vendor. The vendor shall supply a Supplier's Declaration of Conformity (SDoC) 3 to prove their product meets the IPv6 requirements.

FAR Part 11.002(g) states the requirements documents for IT equipment using IP must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. Any exceptions to the use of IPv6 require the Chief Information Officer (CIO) to provide written approval.

Authority

The information directive is issued by the NMB Chief Information Officer, pursuant to the National Mediation Board Delegation Order, dated 05/05/2018.

Additional foundations for this directive include:

- NIST SP 500-267, "A Profile for IPv6 in the U.S. Government – Version 1.0," July 2008
- OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005
- OMB Memorandum (unnumbered), "Transition to IPv6," September 28, 2010
- OMB Memorandum M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)
- CIO Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," July 2012

Directive

This directive implements the requirements of FAR Part 11.002(g) and requires all new NMB acquisitions of IT products or services that use IP to be IPv6 compliant. NMB is implementing these requirements in accordance with the guidance that OMB provided in the September 2010 IPv6 memorandum, and NMB's IPv6 requirements align with the federal goals contained in that document. NMB requirements conform to the overall intent of the U.S. Government (USG) deployment of IPv6 to improve operational efficiency, provide the general public with continued access to citizen services and ensure the government is capable of accessing IPv6-only services.

In accordance with Office of Management and Budget (OMB) memo M-21-07 dated November 19, 2020, by FY2023 all new networked Federal Information systems will be IPv6-enabled at the time of deployment. It is NMB's strategic intent to phase out the use of IPv4 for all systems.

A vendor responding to an RFP for an IT service or product using IP must complete and sign a Suppliers Declaration of Conformity (SDoC), a legal document that specifies and certifies the product's IPv6 capabilities. The Contracting Officer Representative (COR) analyzes the requirements, the IPv6 requirements and the product's capabilities as captured on the SDoC during the technical evaluation of the vendor's proposal, and then the COR sends the analysis to the CO. The COR must notify the CO of all contract specifications that do not comply with providing full feature functionality for IPv6 and act in accordance with the instructions of the CO.

When NMB procures an IT service or product using IP via federal schedule, sole source or credit card, the NMB COR is responsible for obtaining the SDoC from the vendor and creating a procurement package that includes the vendor's SDoC and an analysis between the requirements and the product's capabilities as captured in the SDoC. The COR must submit this procurement package with the PR.

For further information about this memorandum, please contact the National Mediation Board Office of Information Services.