



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

Internet Protocol Version 6 (IPv6) Compliance Policy

1. PURPOSE

To implement the Internet Protocol version 6 (IPv6) compliance requirements for acquiring information technology (IT) products and services contained in Federal Acquisition Regulation (FAR) 11.002.

2. SCOPE

This policy applies to all new EPA acquisitions of IT products or services using Internet Protocol (IP). Additional specifics are found in the IPv6 IT Procurement Checklist.¹

3. AUDIENCE

The audience for this policy includes, but is not limited to, EPA employees seeking to procure a networked IT product or service, vendors responding to Requests for Proposal (RFP) and acquisition staff involved in the procurement process.

4. 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) 500-267.²

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

¹ The IPv6 IT Procurement Checklist is available at https://usepa.sharepoint.com/sites/oei/OTOP/_layouts/15/WopiFrame.aspx?sourcedoc=%7B13848D42-E199-479C-BF5E-3A329B6E2080%7D&file=IPv6%20-%20IT%20Procurement%20Checklist%20final.docx&action=default.

² NIST SP 500-267 is available online at <https://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf>.



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

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, unless they are or will be managed by the Enterprise Services Network. 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. Sufficient details supporting the waiver must be included in the request (e.g., prohibitive cost or scheduling conflicts).

5. AUTHORITY

The information directive is issued by the EPA Chief Information Officer, pursuant to Delegation 1-19, dated 07/07/2005.

Additional legal foundations for the policy include:

- FAR Part 39 – Acquisition of Information Technology
- FAR Part 11.002(g) – Describing Agency Needs – Policy
- 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
- CIO Council, “Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government,” July 2012

6. POLICY

This policy implements the requirements of FAR Part 11.002(g) and requires all new EPA acquisitions of IT products or services that use IP to be IPv6 compliant. EPA is

³ NIST's description of an SDoC is available online at <https://www.nist.gov/sites/default/files/documents/standardsgov/Sdoc.pdf>.



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

implementing these requirements in accordance with the guidance that OMB provided in the September 2010 IPv6 memorandum, and EPA's IPv6 requirements align with the federal goals contained in that document. EPA 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.

A requestor in an EPA office seeking to procure an IT product or service using IP must work with his/her Contracting Officer (CO) to ensure appropriate IPv6 requirements language is included in:

- Procurement Requests (PR)
- Advanced Procurement Plans (APP)
- Statements of Work (SOW)
- Requests for Proposal
- Awarded Contracts

A requestor in an EPA office seeking to procure an IT product or service using IP must complete the IPv6 IT Procurement Checklist. This checklist is a guide to help ensure that products and services that use IP provide full feature functionality in both dual stack (IPv4 and IPv6) and IPv6-only environments in compliance with the NIST USGv6 Testing Program. The requestor provides the IPv6 IT Procurement Checklist to the CO during the RFP development to ensure IPv6 requirements are included in the standard language section of the RFP.

A vendor responding to an RFP for an IT service or product using IP must complete and sign an SDoC, a legal document that specifies and certifies the product's IPv6 capabilities. The requestor 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 requestor sends the analysis to the CO. The requestor 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 EPA procures an IT service or product using IP via federal schedule, sole source or credit card, the EPA requestor is responsible for obtaining the SDoC from the vendor and creating a procurement package that includes the IPv6 IT Procurement Checklist, the vendor's SDoC and an analysis between the requirements and the product's capabilities as captured in the SDoC. The requestor must submit this procurement package to the CO with the PR.

A detailed specification of language and requirements can be found in Interim Policy Notice # 17-01 (Task R – Internet Protocol Version 6 (IPv6))⁴ and the IPv6 IT Procurement Checklist.

Only the EPA CIO may waive the IPv6 requirements and must do so in writing.

⁴ Interim Policy Notice # 17-01 – Use of 22 Cybersecurity Tasks (December 2016) was issued to provide guidance on using specific limited-use cybersecurity tasks in existing and new performance work statements (PWS) and SOWs. Task R contains language associated with IPv6 requirements. It is available on the EPA intranet at http://intranet.epa.gov/oei/saiso/documents/ipn_december_2016.docx.



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

7. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

- Approves or disapproves all IPv6 compliance waivers to this policy.

Director of Office of Information Technology Operations (OITO)

- Receives IPv6 waiver requests.
- Recommends approval/disapproval of IPv6 waiver requests to CIO.

Senior Information Officials (SIO)

- Submit IPv6 waiver requests from their Program Offices or Regions.

EPA Staff Requesting Procurement of IT Product/Service

- Include appropriate IPv6 requirements language in PRs and APPs.
- Work with CO to ensure appropriate IPv6 requirements language is included in SOWs, RFPs and awarded contracts.
- Complete IPv6 IT Procurement Checklist and send to CO.
- Analyze the requirements, the IPv6 requirements and the product's capabilities as captured on the SDoC and submit analysis to CO.
- If procured via federal schedule, sole source or credit card, then obtain SDoC from vendor and submit SDoC to CO.
- Notify CO of all contract specifications that do not comply with providing full feature functionality for IPv6.

Contracting Officers (CO)

- Contracting officers may rely on the requiring activity's declaration on the APP to determine the applicability of IPv6 requirements to its acquisition. When the APP and the requirements documents provided by the requiring activity establish the applicability of IPv6 in accordance with FAR 11.002, the contracting officer shall:
 - (a) Include a contract requirements statement in solicitations that specifically states that products and services that use the Internet Protocol provide full feature functionality in both dual stack (IPv4 and IPv6) and IPv6-only environments in compliance with the NIST USGv6 Testing Program. (See NIST SP 500-267, "A Profile for IPv6 in the U.S. Government – Version 1.0.") The IPv6 requirements statement shall be substantially the same as the statement provided in EPA's contracting writing templates and the IPv6 IT Procurement Checklist; and
 - (b) Include instructions in solicitations that require offerors to notify the contracting officer of any contract specifications that do not comply with providing full feature functionality for IPv6.



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

Vendors

- Complete and sign an SDoC that specifies and certifies the product's IPv6 capabilities and then submit with proposal.

8. RELATED INFORMATION

OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005

<https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-22.pdf>

OMB Memorandum (unnumbered), "Transition to IPv6," September 28, 2010

https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf

NIST SP 500-267, "A Profile for IPv6 in the U.S. Government – Version 1.0," July 2008

<https://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf>

CIO Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," July 2012

https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf

NIST website: "USGv6: A Technical Infrastructure to Assist IPv6 Adoption"

<https://www-x.antd.nist.gov/usgv6/>

FAR Part 11.002(g) – Describing Agency Needs – Policy

https://www.acquisition.gov/sites/default/files/current/far/html/Subpart%2011_1.html#wp1086792

FAR Part 39 – Acquisition of Information Technology

<https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html>

Interim Policy Notice # 17-01 – Use of 22 Cybersecurity Tasks (December 2016)

http://intranet.epa.gov/oei/saiso/documents/ipn_december_2016.docx

IPv6 IT Procurement Checklist

https://usepa.sharepoint.com/sites/oei/OTOP/_layouts/15/WopiFrame.aspx?sourcedoc=%7B13848D42-E199-479C-BF5E-3A329B6E2080%7D&file=IPv6%20-%20IT%20Procurement%20Checklist%20final.docx&action=default

9. DEFINITIONS

Advanced Procurement Plan (APP): A plan that enables program and procurement officials to identify and schedule procurement requirements in advance of needs.



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

Internet Protocol (IP): A protocol that uses datagrams, or data packets, for sending data through networks. Data are encapsulated in packets that contain routing and identity information so that the network knows where the data comes from and where it is supposed to go. Version 4 is the standard Internet Protocol. IPv6 is being adopted by the federal sector and version 4 will be phased out over time.

Internet Protocol version 6 (IPv6): Internet Protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Information Technology (IT): Defined by the Clinger-Cohen Act of 1996, sections 5002, 5141 and 5142, means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. For purposes of this definition, equipment is "used" by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. It does not include any equipment acquired by a federal contractor incidental to a federal contract.

Supplier's Declaration of Conformity (SDoC): A document which shows that a product, process or service conforms to a standard or technical regulation. The supplier provides written assurance of conformity to the specified requirements. This is also sometimes called Self Declaration of Conformity.

U.S. Government v6 Profile (USGv6): A recommended acquisition guide for IPv6 capabilities in common network products. It is meant as a strategic planning guide for USG IT acquisitions to help ensure the completeness, correctness, interoperability and security of early IPv6 product offerings so as to protect early USG investments in the technology.

Abbreviations including acronyms are summarized in *Appendix: Acronyms & Abbreviations*.

10. WAIVERS

A requestor in an EPA office seeking a waiver to procure an IT product or service that does not meet the IPv6 compliance requirements specified in FAR 11.002(g) and in this policy must submit a signed request via memorandum from his/her Senior Information Official (SIO) to the Director of the Office of Information Technology Operations (OITO). All IT procurements for hardware, software and services that do not comply with federal and EPA IPv6 requirements require written approval from the CIO.

11. MATERIAL SUPERSEDED

N/A



INFORMATION DIRECTIVE POLICY

Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

12. CONTACTS

For further information about this policy, please contact the Office of Environmental Information, Office of Information Technology Operations, Director of Enterprise Hosting Division.

Steven Fine
Deputy Chief Information Officer
U.S. Environmental Protection Agency



Internet Protocol Version 6 (IPv6) Compliance Policy		
Directive No.: CIO 2124.0	CIO Approval: 2-13-2018	Transmittal No.: 18-002

**APPENDIX:
ACRONYMS & ABBREVIATIONS**

APP	Advanced Procurement Plan
CIO	Chief Information Officer
CO	Contracting Officer
FAR	Federal Acquisition Regulation
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
NIST	National Institute of Standards and Technology
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
PR	Procurement Request
PWS	Performance Work Statement
RFP	Request for Proposal
SDoC	Supplier's Declaration of Conformity
SIO	Senior Information Official
SOW	Statement of Work
SP	Special Publication
USG	U.S. Government
USGv6	U.S. Government v6 Profile