UNITED STATES OFFICE OF
GOVERNMENT ETHICS

★

Preventing Conflicts of Interest
in the Executive Branch

Internet Protocol Version 6 (IPv6) Policy

Information Technology Division

May 2021

1.0 Review Dates

The Chief Information Officer or his designee must approve any exception to this policy or related procedures.

<u>Document Version Control</u>

Version Number	Created By	Edited By		Date	Description of changes
1.0	*Ty Cooper*	*Ty Cooper*		*2021-05-07*	Initial version

2.0 APPROVAL

This policy is effective on the date signed below.

_____   _____

Ty Cooper, CISSP, CSCP   Date
Chief Information & Cybersecurity Officer

3.0 OVERVIEW

Established by the Ethics in Government Act (October 26, 1978), the United States Office of Government Ethics (OGE) leads and oversees the executive branch ethics program which is at work every day in more than 130 agencies. The executive branch ethics program works to prevent financial conflicts of interest to help ensure government decisions are made free from personal financial bias.

This document, which applies to Internet Protocol Version 6 (IPv6), sets forth OGE's policy related to the Agency's IPv6 deployment and implementation. This policy governs the requirements for completing the operational deployment of IPv6 as well as capturing considerations for transitioning from the current dual-stack IPv4/IPv6 environment in accordance with the Office of Management and Budget (OMB) Memorandum M-21-07 requirements. It defines the governance and support for the ongoing use and future development of IPv6. The Information Technology Division (ITD) is responsible for this policy.

The main advantages of IPv6 are:
- Expanded addressing capability,
- Security extensions for authentication and privacy,
- Flow labeling capability,
- Improved efficiency in routing and packet handling,
- Support for auto-configuration and plug-and-play capabilities,
- Support for embedded IP security,
- Elimination of the need for Network Address Translation (NAT),
- Support for widely deployed routing protocols,
- Network efficiency and bandwidth conservation, and
- Transition and interoperability mechanisms that allow users to deploy IPv6 incrementally.

4.0 REFERENCES AND AUTHORITIES

This Policy is written in accordance with OMB Memo M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, signed November 19, 2020.

5.0 POLICY

No later than the end of Fiscal Year (FY) 2023, all new networked OGE information systems will IPv6-enabled at the time of deployment (the use of IPv6 is "turned on" for production use). This commitment reflects OGE's strategic intent to phase out the use of IPv4 for all systems.

IPv6 Project Team
OGE has established a primary IPv6 governance project team that assesses, prioritizes, and approves requirements that will meet the IPv6 standards. The team, designated as an Agency-wide integrated project team, consists of acquisition, policy, technical, and cybersecurity stakeholders. The group facilitates the IPv6 pilot system and all related activities. Continuous monitoring will be leveraged to support the IPv6 pilot deployment and to identify requirements needed to develop an implementation plan. All transition activities from dual-stack IPv4/IPv6 to full IPv6 must meet OMB-defined timelines and

established Agency IT governance, including enterprise risk management. The group determines further recommendations on IPv6 hardware and software requirements as appropriate.

IPv6 Infrastructure Implementation

The integrated project team must develop an IPv6 implementation plan. This plan includes the update of the Agency's information resource management (IRM) strategic plan with transition details that provide direction regarding processes for new procurements.

Ensuring Adequate Security

OGE shall establish plans to fully support IPv6 services in IT security plans, enterprise architecture, and acquisitions. All systems that support network operations and/or enterprise security services shall be IPv6-capable and operate in IPv6-only environments. OGE shall monitor and manage compliance with all applicable Federal guidance and leverage industry best practices, as appropriate, to secure the deployment and operation of IPv6 networks. All security and privacy policy assessments, authorizations, and monitoring processes shall address the production use of IPv6 in Federal information systems.

Contact

For further information about this policy, please send inquiries to the U.S. Office of Government Ethics, Information Technology Division, Chief Information Officer, at ContactOGE@oge.gov.