EA-04
State CIO Adopted: June 24, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2024

WaTech
Washington Technology Solutions

Replaces:
300: Statewide Migration to IPv6 Policy
December 11, 2017
85.20: ES IP Address Management Standard

INTERNET PROTOCOL VERSION 6 (IPv6)
IMPLEMENTATION POLICY

See Also:
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **All agencies must require that purchases of IT products and services that use the Internet Protocol (IP) are compatible with IPv6.**

2. **All agencies must submit an updated migration plan for IPv6 as part of the annual certification process by September 30, 2024.**

3. **Agencies must share a migration plan reflecting IPv6 compatible equipment lifecycle management as part of the annual certification process by September 30, 2025.**

4. **Agencies must use dual stack IPv4 and IPv6 when both protocols are required for address management. See SP 800-119, Guidelines for the Secure Deployment of IPv6*, para 6.4.***

5. **All agency internal networks must route (Wide Area Network) WAN Internet Protocol version 6 (IPv6) to state managed networks by July 1, 2030.**

6. **All Agencies will implement the following (Local Area Network) LAN connections by July 1, 2040.**

    a. Upgrade public and non-organizational facing servers and services (e.g., web, email, Domain Naming Service (DNS), etc.) to operationally use IPv6.

    b. Upgrade internal client hardware and software that communicates with public internet servers and support enterprise networks to operationally use IPv6 using dual stack.

        i. Agencies must review hardware and software compatibility with IPV6 every six months.

7. **Agencies must acquire their IPv6 address block allocations from WaTech. See Enterprise Service: IP Address Management.**

a. Agencies must create hierarchical addressing schemes that support address summarization and nibble boundaries.

b. WaTech will only route IPv6 addresses that have been allocated to state agencies from WaTech Enterprise Services, as the designated IPv6 Manager for the state. See the NIST SP 800-119, Guidelines for the Secure Deployment of IPv6.

8. **WaTech will provide the IPV6 addresses for public facing external connections or services.**

   a. State Agencies will not use their allocated IPv6 addresses for this purpose.

   b. WaTech will advertise the entire IPv6 / 24 allocation to its ISP's.

   c. Cloud service providers will provide IPV6 addressing for public internet facing connections.

REFERENCES:

1. Enterprise Service: IP Address Management
2. NIST 800-119 Guidelines for the Secure Deployment of IPv6
   a. Para. 3.7.3.3 IPv6-Specific DNS Security Recommendations.
   b. Para 6.4 Dual Stack Ipv4/IPv6 Environments.
      i. RFC 4213 Basic IPv6 Transition Mechanisms.
3. Ref 4: RFC 4193- Global Unique Local Addressing
4. Ref 5: RFC 4890
5. Ref 6: RFC 6177 IPv6 Address Assignment to End Sites
6. Para. 2 On /48 Assignment to End Sites
7. Ref 7: IPv6 Subnet Calculator.
8. NIST Cybersecurity Framework Mapping:
   - Identify.Governance-1 (ID.GV-1): Organizational information security policy is established and communicated.
   - Identify.Supply Chain-3 (ID.SC-3): Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.

CONTACT:

For questions about this policy, please email the policy mailbox.