INTERNET PROTOCOL VERSION 6 CONSIDERATIONS FOR TRUSTED INTERNET CONNECTIONS 3.0

January 2022

INTRODUCTION

The transition of federal networks to Internet Protocol version 6 (IPv6) has been prioritized by the Federal Government since the release of Office of Management and Budget (OMB) Memorandum (M) 05-22, "Transition Planning for IPv6," in 2005.[a] The memorandum calls for agencies to upgrade their infrastructures to use IPv6. In 2020, the Federal Government renewed its focus on IPv6 through the publication of OMB M-21-07: "Completing the Transition to IPv6."[b] The memorandum specifically entrusts the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security (CISA) to enhance the Trusted Internet Connections (TIC) program to support the implementation of IPv6 in federal information technology (IT) systems. In order to support agencies, CISA has issued this TIC 3.0 and IPv6 network guidance to help agencies to secure their networks.

PURPOSE

This guidance reflects the authorities administered to the TIC program, outlined in OMB M-21-07, to enhance relevant security and resilience programs and services to fully support the deployment of IPv6 across federal IT systems. The purpose of this document is to guide federal civilian agencies in supporting IPv6 by:

- Providing IPv6 protocol information to enable a general understanding,
- Informing agencies of their responsibilities concerning OMB M-21-07,
- Aligning TIC 3.0 security objectives and security capabilities to securely support IPv6, and
- Offering awareness and guidance regarding IPv6 security considerations.

This document is intended to be architecture-agnostic and broadly support the government-wide deployment and use of the IPv6 network protocol. It is not intended to be prescriptive but rather facilitate decision-making in determining the appropriate level of security in IPv6 environments.

This document will explain the background of IPv6, list security considerations for the protocol, and provide awareness of IPv6 security features according to TIC guidance. This serves to facilitate conversations surrounding the protocol; additional guidance may be released according to agency needs.

SCOPE

In accordance with OMB M-21-07, federal agencies need to advance IPv6 networks to ensure future growth and innovation in internet services and technology. To keep pace with fast-moving technology, the Federal Government is expanding and enhancing its strategic commitment to IPv6. This document focuses on security considerations for the modernized protocol as they relate to agencies' TIC 3.0 implementation. Agencies must deploy IPv6 to realize the full benefits and security of the protocol across the Federal Government. This guidance directly supports OMB M-21-07.

[a] "Transition Planning for Internet Protocol version 6 (IPv6)," Office of Management and Budget M-05-22 (2005). https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf.
[b] "Completing the Transition to Internet Protocol version 6 (IPv6)," Office of Management and Budget M-21-07 (2020). https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf.

ASSUMPTIONS AND CONSTRAINTS

This section is intended to clarify significant details about the structure and use of this document. The assumptions and constraints for this guidance are outlined below.

- This document applies to networks where IPv6 is deployed; it does not focus on dual-stacked environments.
- This guidance is not intended to be comprehensive and should not be interpreted as a compliance requirement nor reference architecture.
- This guidance is not focused on virtualized environments or IPv6 deployments in the cloud.
- The intent of this document is to specifically address the security considerations related to the use of IPv6 in TIC 3.0 deployments.
- This guidance is not designed as a TIC use case but can be referenced when implementing TIC 3.0 guidance.
- Agencies should reference this IPv6 guidance as a consideration when leveraging the TIC 3.0 Security Capabilities Catalog[c] to frame security capabilities while enabling IPv6 environments.
- While IPv6 has the potential to provide federal agencies with a substantial technological benefit, agencies must understand the security considerations to enable the benefits of this protocol to its full capacity.
- This document is designed to identify potential security impacts in the IPv6 environment to inform agencies' prevention, mitigation, and detection of emerging threats.
- Agencies are required to cooperate to enhance security guidelines for IPv6 adoption throughout the federal IT infrastructure.
- Agencies should be prepared to enhance and maintain their IPv6 deployments in accordance with OMB M-21-07.
- Agencies are encouraged to test products and services utilizing IPv6 to understand their interoperability and backwards compatibility with other network security tools.

PROTOCOL HISTORY

Every device that connects to a network is identified through an internet protocol (IP) address for internet communication. Today, the internet uses two IP address versions—Internet Protocol version 4 (IPv4) and IPv6, but the protocols do not interoperate. Organizations across the public and private sectors maintain distinct network infrastructures, or dual stacks, to accommodate both protocols concurrently.

IPv4 was developed by the Internet Society for the Defense Advanced Research Projects Agency (DARPA) in 1983.[d] IPv4 uses 32-bit addressing which only allows for the creation of just under 4.3 billion (2^{32}) distinct IP addresses. With the exponential adoption of the internet, the pool of IPv4 addresses was exhausted in 2011.[e] Since then, IPv4 has been tightly managed with network address translation (NAT).

Although IPv6 was developed in 1998,[f] it has gained popularity in recent years to address the shortage of IP address assignments available under IPv4. IPv6 uses 128-bit addressing, which allows for approximately 340 undecillion (2^{128}) distinct IP addresses. This address pool is almost 100 octillion (10^{29}) times larger than the address pool for IPv4. IPv6 is not designed to be backward compatible with IPv4, so a dual stack network with both IPv6 and IPv4 can support transitional updates to the network infrastructure.

---

[c] "TIC 3.0 Security Capabilities Catalog," Cybersecurity and Infrastructure Security Agency (October 2021). https://www.cisa.gov/sites/default/files/publications/CISA%20TIC%203.0%20Security%20Capabilities%20Catalog%20v2.0_0.pdf.
[d] Information Sciences Institute, "Request for Comments 791," Internet Engineering Task Force (1981). https://tools.ietf.org/html/rfc791.
[e] "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied," Internet Corporation for Assigned Names and Numbers (2011). https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.
[f] S. Deering and R. Hinden, "Request for Comments 2460," Internet Engineering Task Force (1998). https://tools.ietf.org/html/rfc2460.

This 37-year evolution from IPv4 towards IPv6 is illustrated in Figure 1.

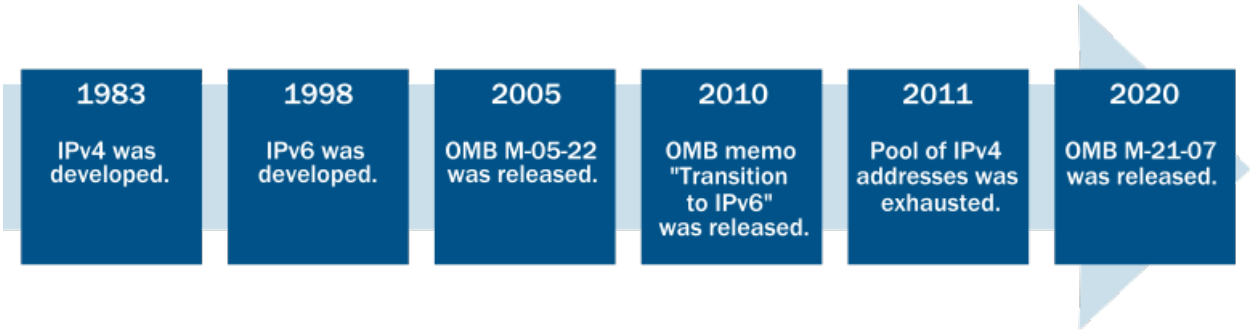

Figure 1: IPv6 Policy Timeline in the Federal Government

To leverage this larger address space, OMB sought to accelerate the transition to IPv6 in the Federal Government with the issuance of OMB M-05-22 in 2005. The memorandum proposed a timeline for agency infrastructure to use IPv6 and agency networks to interface with this modernized IPv6 infrastructure by 2008. Agencies were advised to ensure that all new IT procurements be IPv6-compatible to capitalize on cost-savings. During this stage of transition, all new IP-enabled products procured by agencies were required to interoperate with both IPv4 and IPv6. In 2010, OMB released an updated memorandum, "Transition to IPv6,"[g] listing necessary steps for agencies to expedite operational deployments of IPv6 to enable IT modernization.

Agencies are now being required to move to IPv6-enabled systems and services under OMB M-21-07 to further enhance security. Under the management of the Federal Chief Information Officer (CIO)'s IPv6 Federal Working Group, OMB M-21-07 directs agencies to further enhance security by completing the transition to IPv6-enabled systems and services through a series of milestones outlined in the memo. To support OMB M-21-07, this guidance describes the security considerations for IPv6.

IPv6 is one critical component in enterprise network modernization that allows for increased scalability and enhanced security for network infrastructures. As CISA develops capabilities to secure the Federal Government, the adoption of IPv6 will improve security beyond what is currently provided by IPv4.

PROTOCOL BENEFITS

The Internet Engineering Task Force (IETF) provides specifications for the transmission of datagrams over the internet between source and destination nodes identified by IP addresses.[h] IPv6 was developed to improve upon the address space limitations and other shortcomings of IPv4. Although there are many similarities between IPv4 and IPv6, the following points highlight key differences between the two versions of the protocol.[i]

- **IPv6 provides greater expansion of the IP address space.**
  As discussed above, IPv4's 32-bit address size resulted in IP address issuers exhausting their available IPv4 address allocations in 2011.[j] IPv6 has a 128-bit address size, expanding the number of unique addresses. This should allow for every internet-connected device to have a globally unique IPv6 address well into the foreseeable future.

[g] "Transition to IPv6," Office of Management and Budget (2010). whitehouse.gov/sites/whitehouse.gov/files/omb/assets/egov_docs/transition-to-ipv6.pdf.
[h] Information Sciences Institute, "Request for Comments 791," Internet Engineering Task Force (1981). https://tools.ietf.org/html/rfc791.
[i] S. Deering and R. Hinden, "Request for Comments 2460," Internet Engineering Task Force (1998). https://tools.ietf.org/html/rfc2460.
[j] "Available Pool of Unallocated IPv4 Internet Address Now Completely Emptied," The Internet Corporation for Assigned Names and Numbers (2011). https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf.

- **IPv6 enables the automatic configuration of IP addresses.**
  Unlike IPv4 networks, which require administrators to assign an IP address to hosts or a Dynamic Host Configuration Protocol (DHCP) server to assign those addresses, IPv6 networks are plug-and-play in nature and support automatic address configuration. IPv6-enabled hosts can utilize stateless address autoconfiguration (SLAAC) to generate their own link-local IP addresses using their media access control (MAC) address and information advertised by routers.[k] With IPv6, address assignment is less dependent on a server. DHCP version 6 (DHCPv6) and SLAAC exist to accommodate a network with either all IPv6 hosts or a dual-stack network with a mix of IPv4 and IPv6 hosts.

- **IPv6 offers greater support for header options and extensions.**
  IPv6 simplifies IPv4 headers and provides greater flexibility with the introduction of optional extension headers. These headers provide options for functions such as packet fragmentation, authentication, and mobility. IPv6 optional extension headers are designed to be chained together after the main IPv6 header. The IPv6 packet is depicted in Figure 2.[l]

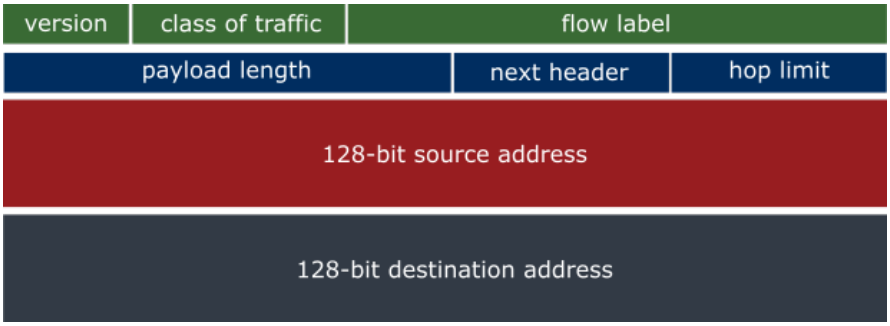

Figure 2: IPv6 Packet

- **IPv6 was designed to support authentication and privacy capabilities.**
  IPv4 was initially developed with minimal security features, and security capabilities were added to the protocol over time. IPv6, on the other hand, was designed with extension headers to support authentication, data integrity, and data confidentiality.

- **Mobile IPv6 is more robust and simpler to manage.**
  Mobile support exists for IPv4, but it is cumbersome to administer and relies on components and processes such as special routers and prearranged security associations. Mobile IPv6 allows mobile hosts to retain their home IP address regardless of their attachment to the internet without depending on those additional technologies and processes.[m]

There are many other differences between IPv4 and IPv6, but the addressing, security, and mobility features are most relevant to federal agencies adopting the TIC 3.0 guidance[n] and OMB M-21-07. The following section provides examples of the protocol's characteristics that agencies should be aware of when implementing TIC 3.0 in IPv6 environments.

[k] S. Thomson, T, Narten and T. Jinmei, "Request for Comments 4862," Internet Engineering Task Force (2007). https://tools.ietf.org/html/rfc4862.
[l] S. Deering and R. Hinden, "Request for Comments 2460," Internet Engineering Task Force (1998). https://tools.ietf.org/html/rfc2460.
[m] C. Perkins, Ed., D. Johnson, and J. Arkko, "Request for Comments 6275," Internet Engineering Task Force (2011). https://tools.ietf.org/html/rfc6275.
[n] "Trusted Internet Connections," Cybersecurity and Infrastructure Security Agency (2021). https://www.cisa.gov/trusted-internet-connections.

PROTOCOL IMPACTS ON TIC 3.0

IPv6 was partly developed to address security concerns that were not factored into the initial creation of IPv4. However, this does not mean that IPv6 is inherently more secure than IPv4. IPv6 has its own operational security concerns[op] and agencies should seek to understand the protocol's effect on their network security architecture. Similarly, agencies should consider how IPv6 networks may affect their adoption of the TIC 3.0 guidance as characteristics of the protocol are expected to impact some network management operations. This section provides an overview of the TIC objectives and security capabilities and a mapping of IPv6 characteristics to the TIC objectives and capabilities.

TIC OBJECTIVES AND SECURITY CAPABILITIES

The overall purpose of the TIC initiative is to standardize and optimize the security of network connections currently in use by the Federal Government. The TIC 3.0 Program Guidebook[q] defines encompassing security objectives intended to set expectations for architectures, guide TIC 3.0 implementation, and establish clear goals at the network level. These objectives can also be used to guide agencies in securing their networks in the IPv6 environment. The possible impacts to TIC objectives related to IPv6 are described in the following section of this document. Table 1 defines the TIC objectives. The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones, stored at either trust zone, or stored at both trust zones.

Table 1: TIC 3.0 Security Objectives

Objectives	Description
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny.
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement.
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit.
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve.
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures.

In addition to the objectives, the TIC 3.0 guidance outlines several security capabilities that describe more tactically the types of security controls that agencies should use to secure their architectures. The TIC security capabilities are composed of two parts:

- Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.
- Policy Enforcement Point (PEP) Security Capabilities: Network-level capabilities that inform technical implementation for relevant use cases.

[o] E. Vyncke, Ed., K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks," Internet Engineering Task Force (2019). https://tools.ietf.org/id/draft-ietf-opsec-v6-18.html.
[p] É. Vyncke, K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks," Internet Engineering Task Force (2021). https://datatracker.ietf.org/doc/html/rfc9099.
[q] "TIC 3.0 Program Guidebook," Cybersecurity and Infrastructure Security Agency (2020). https://www.cisa.gov/publication/tic-30-core-guidance-documents.

PEP capabilities are divided into groups around shared themes, corresponding to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- Domain Name System (DNS),
- Intrusion Detection,
- Enterprise,
- Unified Communications and Collaboration (UCC), and
- Data Protection.

More details on the TIC objectives and security capabilities are provided in the TIC 3.0 Security Capabilities Catalog.

PROTOCOL SECURITY CONSIDERATIONS AND TIC 3.0 MAPPING

The following table provides a high-level summary of IPv6 characteristics that may impact the TIC 3.0 security objectives and capabilities provided in the TIC 3.0 Security Capabilities Catalog. The protocol characteristics, security considerations, and proposed mitigations reflect guidance provided by the IETF and may not represent all issues and security solutions for IPv6 deployments.

The table is intended to help agencies understand how select features of the protocol may affect TIC 3.0 architectures where IPv6 is deployed; it does not focus on dual-stacked environments. It does not offer an exhaustive list of all IPv6 characteristics and security considerations. Agencies should refer to the IETF for detailed information about IPv6 to help determine the protocol's total potential security impact to their organization's network architecture.

Table 2: IPv6 Security Considerations and Relationships to TIC 3.0 Security Objectives and Capabilities

IPv6 Characteristic	Security Consideration	Relationships to TIC 3.0 Security Objectives	Relationships to TIC 3.0 Security Capabilities
Most operators do not have experience running large-scale IPv6 networks.	Operators may not understand the security differences between IPv4 and IPv6. Operators may require training to learn the security considerations for their specific IPv6 deployments.	• Manage Traffic • Protect Traffic Confidentiality • Protect Traffic Integrity • Ensure Service Resiliency • Ensure Effective Response	• Universal: User Awareness and Training
Differences between protocol versions may require policy revisions and parity for PEPs.	Policies created for IPv4 networks may need to be revised for IPv6 networks since differences, such as address structure and header options, may render IPv4-based policies ineffective. Policies should be reviewed, and updated as needed, to ensure policy parity.	• Manage Traffic • Protect Traffic Confidentiality • Protect Traffic Integrity • Ensure Service Resiliency • Ensure Effective Response	• All TIC 3.0 Security Capabilities

IPv6 Characteristic	Security Consideration	Relationships to TIC 3.0 Security Objectives	Relationships to TIC 3.0 Security Capabilities
Expanded address space may create asset management challenges.	IPv6 subnets provide over 340 undecillion (2^{128}) addresses, which makes asset management procedures, that rely on scanning an enumerated list of device addresses, less feasible. Asset discovery scans may need to be executed in a targeted manner on IPv6 networks to confine the scanning to more manageable ranges of addresses.[r] Agencies need to consider the risk of infeasibility of scanning.	• Manage Traffic • Protect Traffic Confidentiality • Protect Traffic Integrity • Ensure Service Resiliency • Ensure Effective Response	• Universal: Inventory; Configuration Management; Situational Awareness • Web PEP: All web capabilities • Network PEP: Access Control
Multiple addresses and address expression variability may create correlation challenges.	A device may have multiple IPv6 addresses, and an IPv6 address can be expressed by more than one-character string. This can produce correlation problems as a device may be represented in different logs with different addresses. Network administrators should consider logging only devices' canonical IP addresses and correlating those addresses against the data-link addresses stored in the Neighbor Discovery cache to correlate device addresses.	• Manage Traffic • Ensure Effective Response	• Universal: Central Log Management and Analysis; Inventory; Auditing and Accounting • Web PEP: Domain Reputation Filter • Enterprise PEP: Security Orchestration, Automation, and Response
Site-to-site traffic may route across the internet instead of through virtual private network (VPN) tunnels.	The ability for IPv6-addressed devices to directly communicate with each other between trust zones (due to globally unique addresses) means it is possible for site-to-site traffic to be exchanged without passing through a VPN tunnel should the tunnel drop. This could make traffic vulnerable to eavesdropping and injection attacks. PEPs can be configured to help prevent devices at different sites from communicating with each other using unsanctioned paths.	• Protect Traffic Confidentiality • Protect Traffic Integrity • Ensure Service Resiliency	• Universal: Secure Administration; Resilience • Web PEP: Data Loss Prevention • Files PEP: Data Loss Prevention • Email PEP: Data Loss Prevention • UCC PEP: Data Loss Prevention • Data Protection PEP: Data Loss Prevention • Enterprise PEP: Virtual Private Network • Networking PEP: Network Segmentation

[r] F. Gont, T. Chown, "Network Reconnaissance in IPv6 Networks," Internet Engineering Task Force (2016). https://datatracker.ietf.org/doc/html/rfc7707

IPv6 Characteristic	Security Consideration	Relationships to TIC 3.0 Security Objectives	Relationships to TIC 3.0 Security Capabilities
Temporary addresses may create access control list (ACL) management challenges.	The SLAAC protocol's privacy extensions allow for a device to periodically generate a new, temporary IP address to make tracking the device more challenging[s]. The recurring generation of new addresses may make ACL management more demanding as lists may require more frequent updates. Utilizing stable privacy addresses, or assigning addresses manually or via DHCPv6, may ameliorate ACL management challenges.	• Manage Traffic	• Networking PEP: Access Control; Internet Address Denylisting
Temporary addresses may require more frequent fetches of address logs for auditing purposes.	Routers may cache high volumes of addresses when the SLAAC protocol's privacy extensions are utilized to produce temporary addresses. Consequently, the contents of the neighbor cache will need to be fetched at a frequency that ensures all addresses are retrieved and stored for auditing and forensics activities. Exhausting the neighbor cache will cause potential issues with log accuracy and correlation.	• Manage Traffic • Ensure Service Resiliency • Ensure Effective Response	• Universal: Central Log Management with Analysis; Auditing and Accounting; Incident Response Planning and Incident Handling; Resilience • Web PEP: Bandwidth Control • Resiliency PEP: Distributed Denial of Service Protections
Automatic addressing is vulnerable to Denial-of-Service (DoS) attacks.	SLAAC utilizes the Neighbor Discovery Protocol (NDP) to determine a device's link-local address[t]. NDP DoS attacks can occur intentionally, or unintentionally, when a router is overwhelmed by address resolution requests. This is a concern in IPv6 networks due to the large size of IPv6 subnets. NDP DoS attacks may be mitigated by activities such as limiting addresses to a small range of a subnet and controlling the rate at which addresses are assigned to devices[u]. Administrators may also mitigate neighbor discovery cache exhaustion by assigning a unique IPv6 prefix to each host, however this approach may impair privacy if prefixes are not periodically changed or randomized.[v]	• Ensure Service Resiliency • Ensure Effective Response	• Universal: Resilience; Incident Response Planning and Incident Handling; Resilience • Web PEP: Bandwidth Control • Resiliency PEP: Distributed Denial of Service Protections

[s] F. Gont, S. Krishnan, T. Narten, R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6," Internet Engineering Task Force (2021). https://datatracker.ietf.org/doc/html/rfc8981.
[t] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Request for Comments 4861," Internet Engineering Task Force (2007). https://tools.ietf.org/html/rfc4861.
[u] I. Gashinsky, J. Jaeggli, and W. Kumari, "Request for Comments 6583," Internet Engineering Task Force (2012). https://tools.ietf.org/html/rfc6583.
[v] J. Brzozowski, G. Van de Velde, and Nokia, "Request for Comments: 8273," Internet Engineering Task Force (2017). https://datatracker.ietf.org/doc/html/rfc8273.

IPv6 Characteristic	Security Consideration	Relationships to TIC 3.0 Security Objectives	Relationships to TIC 3.0 Security Capabilities
Router advertisements (RAs) may be spoofed and make traffic vulnerable to eavesdropping.	NDP utilizes router advertisements, which are vulnerable to spoofing. Networks should be configured utilizing router advertisement guard (RA guard) to help protect against spoofing attacks[w]. RA guard recommends a process for the dynamic discovery of IPv6 routers, but administrators are encouraged to periodically review the automatically generated list to ensure it is consistent with the expected valid router list. This recommendation also applies to DHCPv6 as RA messages are used to discover default router(s) and on-link prefix determinations.	• Manage Traffic • Protect Traffic Confidentiality	• Universal: Configuration Management; Inventory; Auditing and Accounting • Enterprise PEP: Shadow Information Technology Detection
Manually addressed hosts may be vulnerable to rogue DHCPv6 server attacks.	Rogue DHCPv6 servers may send packets containing malicious IP address assignments to devices. The adoption of these addresses may render hosts vulnerable to on-path attacks. Networks should be configured in accordance with DHCPv6-Shield filtering rules to help ensure devices receive DHCPv6 packets on authorized ports and malicious packets are dropped and logged[x].	• Protect Traffic Confidentiality • Protect Traffic Integrity	• Universal: Configuration Management; Secure Administration • File PEP: Data Loss Prevention • Web PEP: Data Loss Prevention • Data PEP: Data Loss Prevention
DHCPv6 lease files may not be reliable for IP address mapping and auditing purposes.	DHCPv6 utilizes a DHCP Unique Identifier (DUID) to identify devices, as opposed to only the hardware address used for DHCP with IPv4. The DUID may reflect the data-link address for any interface on the device or may be the data-link layer address; some data-link layer addresses are prepended with time information or an opaque number which is less useful for operational security. Moreover, when the DUID is based on the data-link address, this address can represent any interface of the client (e.g., the wireless interface while the client uses its wired interface to connect to the network).	• Ensure Effective Response	• Universal: Central Log Management with Analysis; Configuration Management; Auditing and Accounting

[w] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, and J. Mohacsi, "Request for Comments 6105" Internet Engineering Task Force (2011). https://tools.ietf.org/html/rfc6105.
[x] F. Gont, W. Liu, and G. Van de Velde, "Request for Comments 7610," Internet Engineering Task Force (2015). https://tools.ietf.org/html/rfc7610.

IPv6 Characteristic	Security Consideration	Relationships to TIC 3.0 Security Objectives	Relationships to TIC 3.0 Security Capabilities
Improper extension headers may impair the availability of PEPs.	Packets that do not conform to the recommended extension header order or maximum number of extension header repetitions can confuse and crash PEPs. PEPs should be configured to drop nonconforming packets or enforce the recommended header order and number of repetitions specified by IPv6.	• Ensure Service Resiliency • Ensure Effective Response	• Universal: Resilience; Incident Response Planning and Incident Handling • Web PEP: Bandwidth Control • Resiliency PEP: Distributed Denial of Service Protections

CONCLUSION

IPv6 is an essential component to enterprise network modernization that requires an increased understanding to fully leverage. Like any technology, IPv6 does not exist without its security risks. As the TIC program continues to identify and evolve the security capabilities to secure the .gov, additional modernization and technology areas may be identified to guide the Federal Government. IPv6 offers a wide variety of benefits that opens opportunities to leverage other emerging technologies and concepts. TIC guidance will aid agencies in following OMB guidance as the Federal Government continues to drive towards modernization. The provided guidance is only an initial consideration for agencies. IPv6 can affect other areas of an enterprise which may be covered in future guidance.