Trusted Internet Connections (TIC) 3.0

Response to Comments on the "IPv6 Considerations for TIC 3.0" Guidance

Introduction

In January 2022, CISA released the finalized version of guidance, Internet Protocol version 6 (IPv6) Considerations for TIC 3.0, in accordance with the Office of Management and Budget (OMB) Memorandum (M) 21-07. Since its draft release in September 2021, CISA has completed a comprehensive analysis of comments received on the guidance.

The IPv6 Considerations for TIC 3.0 guidance is intended to be a starting point for agencies to implement IPv6 securely. It is intended to be architecture-agnostic and to broadly support the government-wide deployment and use of the IPv6 network protocol. This fact sheet explains the background of IPv6, lists security considerations for the protocol in relation to the TIC 3.0 security capabilities, and provides awareness of IPv6 security features according to the TIC guidance.

TIC 3.0 Documentation

Core Guidance
Program Guidebook
Reference Architecture
Security Capabilities Catalog
Use Case Handbook
Overlay Handbook

Use Cases
Traditional TIC
Branch Office
Remote User

Other
Pilot Process Handbook
IPv6 Considerations for TIC 3.0

On behalf of OMB, the General Services Administration (GSA), and the Federal Chief Information Security Officer (CISO) Council TIC Subcommittee, CISA thanks all commenters for the critical feedback and questions that allow the guidance documentation to be more effective for each federal agency. CISA reviewed and adjudicated stakeholder comments from the public comment period. The comprehensive review inspired further developments of the guidance.

The feedback is crucial to ensure the guidance fully addresses security considerations for the modernized protocol related to agencies' TIC 3.0 implementation. The input allows the TIC program to better develop the guidance so that it is applicable to federal agencies broadly.

CISA considered each comment independent of the commenter and organization. CISA collaborated with the Federal IPv6 Task Force to understand the feedback and update the documentation appropriately. CISA identified themes from the collected comments and applied them to areas within the documentation that would improve the application of the guidance to agencies and service providers.

Comment Themes

Overall, CISA highlighted four key themes from the comments and responses spanning across the documentation. Commenters wanted further clarification on—or a better understanding of—the following topics.

Updates in Industry Best Practices

Commenters flagged updates in industry best practices for inclusion. CISA updated the document to reflect the most current IPv6 best practices and considerations.

Inclusion of IPv6 Standards

Commenters requested federal standards for implementing specific facets of IPv6 (e.g., stateless address autoconfiguration (SLAAC), Dynamic Host Configuration Protocol version 6 (DHCPv6), and asset management). CISA recognizes the need for additional IPv6 guidance and is collaborating with the Federal IPv6 Task Force to address it.

Scope for the Guidance

Commenters sought specific considerations for dual-stack environments and implementing IPv6 in the cloud. Although out of scope for this documentation, these comments may be considered for future CISA guidance.

Specific Implementation Guidance

Commenters requested additional guidance on implementing IPv6 and TIC 3.0. CISA updated the documentation to reflect new TIC 3.0 security capabilities; however, the documentation was designed to be high-level, so specific guidance, such as use cases, is out of scope. These comments may be considered for future TIC guidance.

Conclusion

CISA anticipates the "IPv6 Considerations for TIC 3.0" guidance will better address stakeholder needs and concerns. CISA is committed to supporting agencies and continuously receiving feedback to aid in developing future iterations of TIC guidance.