Trusted Internet Connections (TIC) 3.0

Response to Comments on the TIC 3.0 Remote User Use Case

Introduction

On October 7, 2021, CISA released a finalized version of the TIC 3.0 Remote User Use Case in accordance with the Office of Management and Budget (OMB) Memorandum (M) 19-26. Since its draft release in December 2020, CISA has reviewed comments from multiple stakeholders. CISA completed a comprehensive analysis on the application of this use case for federal agencies.

This use case defines network and multi-boundary security guidance for agencies that allow users to work remotely. These users could be personnel working from home, connecting from a hotel, or telecommuting from a non-agency-controlled location. This use case deprecates the TIC 3.0 Interim Telework Guidance, published in April 2020 to support the maximized telework posture caused by COVID-19. Collectively, the TIC 3.0 guidance is key in offering flexibility to agencies that are modernizing and securing the connections between the internet, agencies, the cloud, and mobile (remote) users.

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, CISA, and the General Services Administration (GSA), CISA wants to thank all commenters for the crucial feedback and questions that allow the guidance documentation to be more effective for each federal agency. CISA reviewed and adjudicated several comments from the January 2021 request for comments (RFC) period and from stakeholder input throughout 2020. The comprehensive review inspired further developments to the core guidance, namely the Security Capabilities Catalog.

The feedback greatly benefits the guidance and ultimately the updated TIC program. The feedback is critical to making sure TIC 3.0 enhances agency enterprise network security by being broadly applicable to all federal agencies. It also enables the federal government to leverage vendors' capabilities and apply TIC 3.0 effectively.

CISA considered each comment independent of the commenter and organization. CISA collaborated with OMB and GSA to understand the feedback, determine how to modify the TIC 3.0 guidance, and apply the changes appropriately to the documents. CISA identified themes from the collected comments and applied them to areas within the documentation that would improve the application of TIC guidance to agencies and service providers.

Comment Themes

Overall, four key themes, in no specific order, were highlighted from the comments and responses for this document. Commenters wanted further clarification on, or a better understanding of, the following topics.

Clarifications on Telemetry

Commenters requested clarification on when to send telemetry to CISA. The use case was updated to include recent changes in CISA telemetry requirements, specifically in reference to Executive Order 14028 on Improving the Nation's Cybersecurity.

Security Capability Clarification

Commenters sought clarification on the application of specific security capabilities in this use case. This use case was updated to include additional guidance on certain security capabilities.

Orientation towards Zero Trust

Commenters recommended adjusting the use case to have a stronger focus on zero trust, by including steps towards Zero Trust Architecture or making this a Zero Trust Use Case. This use case was updated to include clarifying language, and CISA will coordinate with OMB and the Federal Chief Information Security Officer (FCISO) Council on potentially developing a Zero Trust Use Case.

Scope for the Use Cases

Commenters requested information on topics related to potential future TIC guidance, such as expanding definitions, aligning security capabilities to other cybersecurity guidance, and including new security patterns. While out of scope for this use case, these comments may be considered for future TIC guidance, including the Cloud Use Case.

Conclusion

CISA anticipates the core TIC 3.0 guidance will better address stakeholder needs and concerns. The guidance is expected to evolve to reflect technological advancements, changes in threats, and the lessons learned from TIC pilots to help ensure its usefulness to federal agencies. CISA is committed to supporting agencies and continuously receiving feedback to aid in the development of future iterations of TIC guidance.