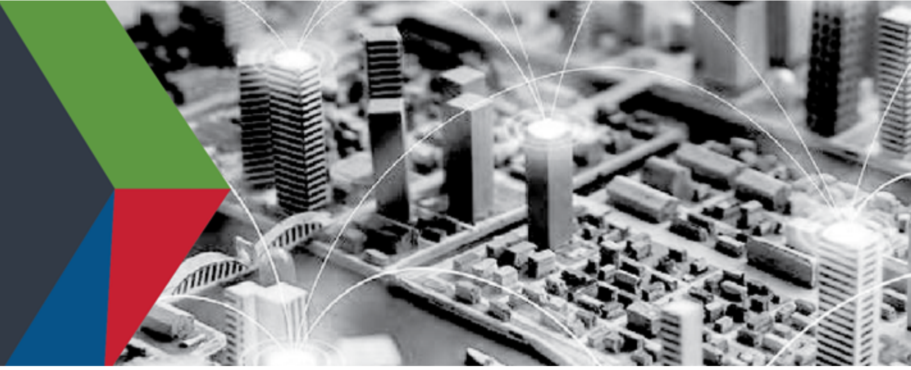
DEFEND TODAY, SECURE TOMORROW



Trusted Internet Connections (TIC) 3.0

Response to Comments on the TIC 3.0 Traditional TIC Use Case and TIC 3.0 Branch Office Use Case

Introduction

On April 7, 2021, CISA released finalized versions of the TIC 3.0 Traditional TIC Use Case and TIC 3.0 Branch Office Use Case in accordance with the Office of Management and Budget (OMB) Memorandum (M) 19-26. Since their draft release on December 20, 2019, CISA has reviewed comments from multiple stakeholders. CISA completed a comprehensive analysis on the application of the use cases for federal agencies while finalizing the use cases.

The use cases are the first of their kind to be finalized for the TIC program since the release of the finalized TIC 3.0 core guidance documents on July 31, 2020. 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 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 (draft)

Other
Pilot Process Handbook

On behalf of OMB, the General Services Administration (GSA), and CISA, CISA wants to thank 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 several comments from the January 2020 request for comments (RFC) period and by stakeholders throughout 2020. The comprehensive review inspired further developments to the core guidance and additional changes that will affect all TIC use cases going forward.

The feedback greatly benefits the guidance and ultimately the updated TIC program. The feedback is crucial to making sure TIC 3.0 enhances agency enterprise network security. The feedback allows the TIC program to understand how the use cases need to be developed to broadly apply 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, three key themes, in no order, were highlighted from the comments and responses for all documents. Commenters wanted further clarification on or a better understanding of the following topics.

Clarifications on Trust Zones, Trust Levels, and Risk Tolerances

Commenters sought additional guidance on trust zones, including trust level determinations and risk tolerance.

Clarifications on Security Capabilities

Commenters looked for additional guidance on security capabilities and capability deployment, including details related to the network segmentation, multi-factor authentication (MFA), and domain name system (DNS) security capabilities.

Scope for the Use Cases

Commenters looked for guidance on topics related to potential future use cases. These comments, while out of scope for the Traditional TIC Use Case and Branch Office Use Case, will bolster candidate future use cases, such as partner network, zero trust, multi-cloud, and remote user.

Alignment to CISA Programs

Commenters sought clarification on topics for other CISA programs, including National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM).

Changes were made throughout the TIC 3.0 core guidance documents based on comments for the Traditional TIC Use Case and Branch Office Use Case. Updates were made to concepts, additional context was added to the assumptions and constraints, and more details were provided on security capabilities. Call-out boxes and emphasized text were added to clarify the scope of the use case and to highlight that agencies have flexibility to determine trust zones and levels. Some of these changes necessitated the update of related documents to maintain consistency. Thus, a new version of the TIC 3.0 Security Capabilities Catalog was released with the finalized use cases.

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.