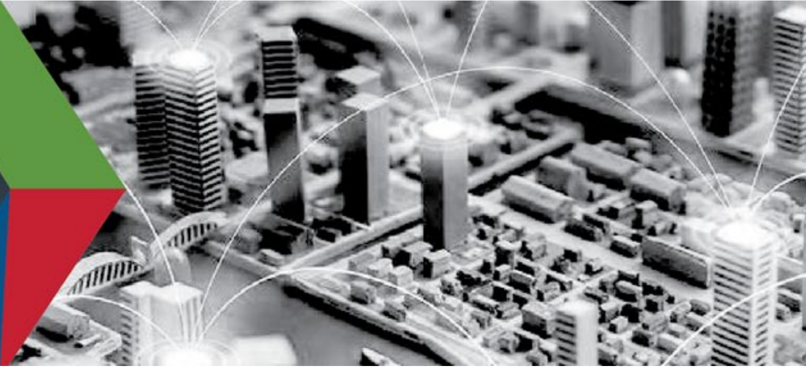

DEFEND TODAY, SECURE TOMORROW

Trusted Internet Connections (TIC) 3.0

Response to Comments on Draft TIC 3.0 Guidance Documentation

Introduction

On July 31, 2020, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) delivered three of the updated and adjudicated TIC 3.0 core guidance documents in response to Office of Management and Budget (OMB) Memorandum (M) 19-26. The guidance documentation is key in offering flexibility while modernizing and securing the connections between the internet, agencies, the cloud, and mobile users.

On December 20, 2019, CISA released eight draft documents as TIC 3.0 guidance for public comments. A request for comments (RFC) period was opened to provide the public with the opportunity to provide their perspectives on the new guidance. Over the seven weeks following the release, approximately 30 combined government and industry organizations sent comments to CISA.

TIC 3.0 Documentation

Core Guidance
Program Guidebook
Reference Architecture
Security Capabilities Catalog[1]
Use Case Handbook*
Overlay Handbook[2]*

Use Cases
Traditional TIC*
Branch Office*

Other
Pilot Process Handbook

**Final version expected late Summer 2020*

On behalf of OMB, the General Services Administration (GSA), and DHS 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 received nearly 500 comments and questions through email, an online repository, and speaking engagements from 14 agencies, eight vendors, one trade association, and seven individuals during the RFC period.

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 service providers' 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.

[1] Formerly known as the Security Capabilities Handbook

[2] Formerly known as the Service Provider Overlay Handbook

Comment Themes

Overall, five key themes, in no order, were highlighted from the comments and responses for all documents. Commenters wanted further clarification or better understanding on the following topics.

Interactions and alignment across the TIC program, other CISA programs, and federal programs:
CISA has added more context and clarity on the interactions and alignment of the TIC program with other CISA and federal programs. CISA has updated Section 14 of the Program Guidebook with additional clarity and added a new section for the National Cybersecurity Protection System (NCPS). NCPS has also updated the NCPS Cloud Interface Reference Architecture.

Amount of support CISA intends to provide to agencies for the TIC guidance and processes:
CISA plans to offer templates, working groups, webinars, and roadshows as needed to explain the TIC guidance and processes. CISA maintains a web page that hosts frequently asked questions (FAQ) and the documents for public access.

Concepts and the terminology articulated in the TIC documentation:
CISA has added more details to the terms and diagrams in the Program Guidebook and Reference Architecture. Additional context has also been added throughout the documents as needed to provide more details on the concepts.

Development, schedule, and authority of the use cases:
The Pilot Process Handbook and Use Case Handbook describe the process, development, and authority of the use cases. OMB M-19-26 specifies the Traditional TIC Use Case, cloud use cases, the Agency Branch Office Use Case, and the Remote Users Use Case. Other use cases have been proposed and will be considered in coordination with OMB, GSA, and the Federal Chief Information Security Officer (CISO) Council.

Additional use cases being proposed for the future of the TIC program:
Several additional use cases have been proposed to CISA. CISA will coordinate with OMB, GSA, and the Federal CISO Council to prioritize and determine use cases to support after releasing the Traditional TIC Use Case and the Branch Office Use Case.

The updated TIC guidance employs new architectural and security concepts to be more supportive of the latest technology and broad range of agency enterprises that will be adopting TIC 3.0. Agencies have accepted the new approach to TIC implementation, and the TIC program has received positive feedback on its increased flexibility and responsiveness to agency needs. Additionally, the number of security capabilities has increased to reflect the growing number of cybersecurity threats and adoption of cloud-based services.

Document-Specific Comments

Prevailing themes were identified for each document and are described below. The themes were addressed within each of the respective documents.

Program Guidebook

Commenters looked for clarity on cross program coordination across the TIC program, Continuous Diagnostics and Mitigation (CDM), NCPS, the former National Cybersecurity and Communications

Integration Center (NCCIC), FedRAMP, and others; clarity on the key terms; and clarity on the roles and responsibilities of the key authorities.

Reference Architecture

Commenters looked for clarity on the relationship between TIC 3.0 and zero trust networking; more information on the prerequisites, boundaries, and criteria of trust zones; and clarity on trust inheritance in traffic between zones and policy enforcement points (PEPs).

Security Capabilities Catalog

The Security Capabilities Catalog, formerly the Security Capabilities Handbook, was renamed to better reflect the updated content. Commenters looked for clarity on which, if any, of the TIC 3.0 capabilities are required; for CISA to include additional proposed capabilities including protections at the operating system and application levels, encryption at rest and in transit, logging, allowlist, and others; and for clarity on what TIC 2.0 capabilities and existing traditional agency deployments can be inherited.

Overlay Handbook*

The Overlay Handbook, formerly the Service Provider Overlay Handbook, was renamed to reflect changes that allow for guidance to apply to overlays produced by agencies or vendors. Commenters look for CISA to standardize the use of the terms “service provider,” “cloud service provider,” and “specific cloud vendor”; to clarify that some mappings may be incomplete and clarify the strength; and to be clearer on the intention of overlays—whether they represent an “approved product list” and how often they would be updated.

Use Case Handbook*

Commenters looked for CISA to be clearer on use case requirements, relationships and data flows between trust zones, and capability deployment. Commenters also wanted clarity on how “real world” networks align with use cases such as the scoping around cloud service providers (CSPs), PEPs, and trust levels.

Traditional TIC Use Case*

Commenters looked for CISA to be clearer on how the use case covers existing inbound and outbound traffic at the agency network. Commenters also wanted clarity on whether existing TIC 2 compliant deployments can be considered as the Traditional TIC Use Case.

Branch Office Use Case*

Commenters looked for CISA to be clearer on how the use case covers existing traffic at the branch office perimeter, including connections to new environments.

Pilot Process Handbook

Commenters looked for CISA to be clearer on whether approved pilots can be used broadly or new pilots are needed after initial approval; be clearer on the relationship between pilots and use cases and which results in the other; and be clearer on the proposal templates, how proposals are assessed, and what the relationship is between the Federal CISO Council and CISA.

**Final version expected late Summer 2020*

Conclusion

CISA anticipates the final 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 also committed to supporting agencies and continuously receiving feedback to aid in the development of future iterations of TIC guidance.