TRUSTED INTERNET CONNECTIONS (TIC)

Response to Comments on the "TIC 3.0 Cloud Use Case"

APRIL 13, 2023

INTRODUCTION

In April 2023, the Cybersecurity and Infrastructure Security Agency (CISA) released the finalized version of TIC 3.0 Cloud Use Case, which is the last of the "Initial Common TIC Use Cases" outlined in the Office of Management and Budget (OMB) Memorandum (M) 19-26. Since the draft release in June 2022, CISA has completed a comprehensive analysis of comments received on the guidance.

The purpose of the Trusted Internet Connections (TIC) initiative is to enhance network security across the federal government. The newest iteration of CISA's TIC guidance is the Cloud Use Case, which provides guidance on applying network and multi-boundary security for agencies that that operate in cloud environments.

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
Cloud

Other
Pilot Process Handbook
IPv6 Considerations for TIC 3.0

FEEDBACK

CISA thanks all commenters for their critical feedback and questions. CISA reviewed and adjudicated stakeholder comments from the public comment period and identified several themes among the comments. The comprehensive review and analysis of the comments inspired further developments of the guidance.

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

COMMENT THEMES

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

- **Risk and Deployment Considerations:** Commenters highlighted concerns that the Draft TIC 3.0 Cloud Use Case implied cloud deployments were riskier than on-premises deployments. CISA modified text in Section 4.2.2 "Risk and Deployment Considerations" to clarify that moving from on-premises to cloud requires a "changes in agency policies and procedures." CISA also tried to include "opportunities for improvement of cybersecurity posture" throughout the document.
- **TIC 3.0 and Zero Trust Inconsistency:** Commenters pointed out inconsistencies with TIC 3.0 and Zero Trust, or they wanted more Zero Trust guidance. CISA added references to Cyber Executive Order 14028, OMB M-22-09 Federal Zero Trust Strategy, Zero Trust Maturity Model, and others throughout the TIC Use Case and updated some capability guidance, as appropriate.
- **Cloud-to-Cloud Connections:** Commenters inquired if Cloud-to-Cloud connections were in scope. CISA added new Agency Cloud Service to Agency Cloud Service, Section 4.3.6, Security Pattern 6. CISA also added a new trust zone ("Additional Agency Cloud Service") in the Conceptual Architecture (Figure 3) to support this new pattern.
- **TIC Compliance:** Commenters wanted a greater emphasis and guidance for compliance. CISA would like to stress that there are no mandatory requirements unique to TIC 3.0. CISA added text to call out opportunities for using cloud solutions to automate policy compliance verification.

- **Protective Domain Name System (DNS) Service:** Commenters asked questions about CISA's new Protective DNS service. CISA would like to highlight that since the release of the Draft TIC Cloud Use Case, CISA has introduced a Protected DNS Resolver Service for Federal Agencies in September 2022. CISA recommends retiring E^{3}A Domain Name Protections from the *TIC Security Capabilities Catalog.*
- **Web and Services Policy Enforcement Points (PEPs):** Commenters asked for clarification, more guidance, and better fidelity with regards to the different uses for the "Web" and "Services" PEPs. CISA modified the Web and Services sections (sections 4.4.2.2 and 4.4.2.10) explaining their intended role in the Cloud context.
- **New Security Capabilities:** Commenters proposed two new PEP capability groups, five new Universal PEP Security Capabilities, and 34 new PEP security capabilities. CISA added several new capabilities to both Universal and PEP Security Capabilities in the new version of the TIC Security Capabilities Catalog.

CONCLUSION

CISA anticipates the TIC 3.0 Cloud Use Case will better address stakeholder needs and concerns. CISA is committed to supporting agencies and continuously receiving feedback to improve its offerings.