Trusted Internet Connections 3.0

TIC Core Guidance Volume 4:

Use Case Handbook

July 2021

Version 1.1

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Revision History

The version number will be updated as the document is modified. This document will be updated as needed to reflect modern security practices and technologies.

Table 1: Revision History

Version	Date	Revision Description	Section/Pages Affected
Draft	December 2019	Initial Release	All
1.0	November 2020	Response to RFC Feedback	All
1.1	July 2021	Updated branding and graphics. Minor grammatical corrections.	All

Reader's Guide

The Trusted Internet Connections (TIC) initiative is defined through key documents that describe the directive, the program, the capabilities, the implementation guidance, and capability mappings. Each document has an essential role in describing TIC and its implementation. The documents provide an understanding of how changes have led up to the latest version of TIC and why those changes have occurred. The documents go into high-level technical detail to describe the exact changes in architecture for TIC 3.0. The documents are additive; each builds on the other like chapters in a book. As depicted in Figure 1, the documents should be referenced in order and to completion to gain a full understanding of the modernized initiative.

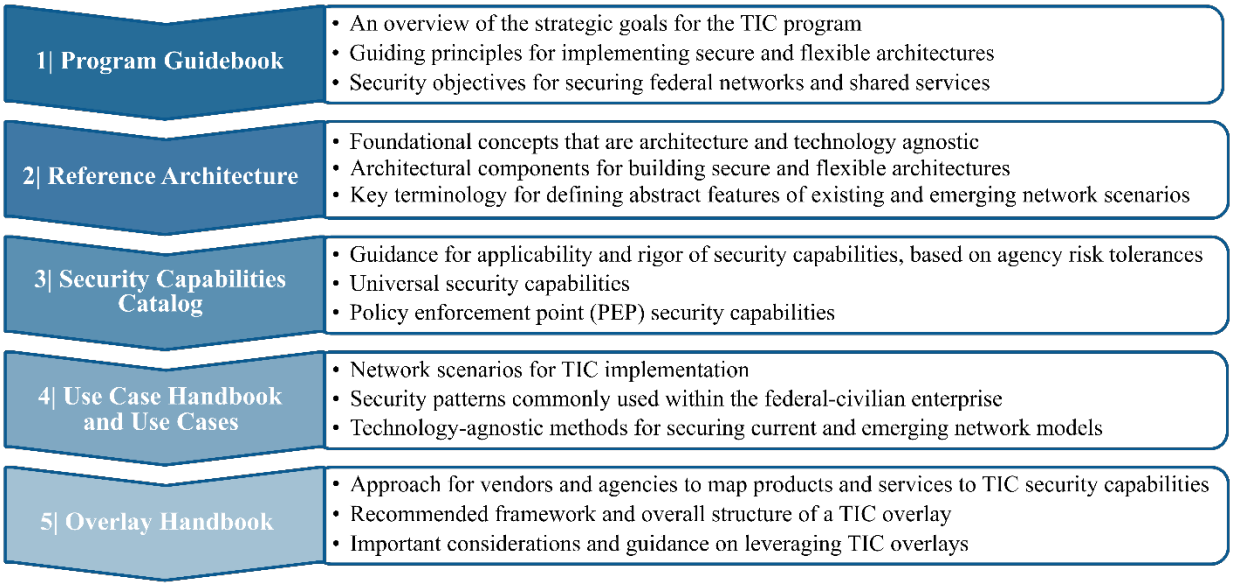

Figure 1: TIC 3.0 Guidance Snapshot

TIC 3.0 Use Case Handbook

Table of Contents

List of Figures

List of Tables

1. Introduction

Trusted Internet Connections (TIC), originally established in 2007, is a federal cybersecurity initiative intended to enhance network and perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative through a robust program that sets guidance and an execution framework for agencies to implement a baseline perimeter security standard.

The initial versions of the TIC initiative sought to consolidate federal networks and standardize perimeter security for the federal enterprise. As outlined in OMB Memorandum (M) 19-26: *Update to the Trusted Internet Connections (TIC) Initiative*[1], this modernized version of the initiative expands upon the original to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications.

1.1 Key Terms

To avoid confusion, terms frequently used throughout the TIC 3.0 documentation are defined below. Some of these terms are explained in greater detail throughout the TIC 3.0 guidance. A comprehensive glossary and acronyms list with applicable attributions can be found in Appendix A.

Boundary: A notional concept that describes the perimeter of a zone (e.g. mobile device services, general support system (GSS), Software-as-a-Service (SaaS), agency, etc.) within a network architecture. The bounded area must have an information technology (IT) utility.

Internet: The internet is discussed in two capacities throughout TIC documentation.

1. A means of data and IT traffic transport.
2. An environment used for web browsing purposes, hereafter referred to as "Web."

Managed Trusted Internet Protocol Services (MTIPS): Services under GSA's Enterprise Infrastructure Solutions (EIS) contract vehicle that provide TIC solutions to government clients as a managed security service. It is of note that the EIS contract is replacing the GSA Networx contract vehicle that is set to expire by Fiscal Year (FY) 2023.

Management Entity (MGMT): A notional concept of an entity that oversees and controls security capabilities. The entity can be an organization, network device, tool, service, or application. The entity can control the collection, processing, analysis, and display of information collected from the policy enforcement points (PEPs), and it allows IT professionals to control devices on the network.

Policy Enforcement Point (PEP): A security device, tool, function, or application that enforces security policies through technical capabilities.

Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).[2] Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

[1] "Update to the Trusted Internet Connections (TIC) Initiative," Office of Management and Budget M-19-26 (2019). https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf.
[2] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

Telemetry: Artifacts derived from security capabilities that provide visibility into security posture.

TIC: The term "TIC" is used throughout the Federal Government to denote different aspects of the TIC initiative; including the overall TIC program, a physical TIC access point (also known as a Traditional TIC), and a TIC Access Provider (TICAP – see below). This document refers to TIC as an adjective or as the Trusted Internet Connections initiative.

TIC Access Point: The physical location where a federal civilian agency consolidates its external connections and has security controls in place to secure and monitor the connections.

TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

TIC Overlay: A mapping of products and services to TIC security capabilities.

TIC Use Case: Guidance on the secure implementation and/or configuration of specific platforms, services, and environments. A TIC use case contains a conceptual architecture, one or more security pattern options, security capability implementation guidance, and CISA telemetry guidance for a common agency computing scenario.

Trust Zone: A discrete computing environment designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.

Web: An environment used for web browsing purposes. Also see Internet.

2. Purpose of the Use Case Handbook

The *TIC 3.0 Use Case Handbook* (Use Case Handbook) describes the content and format of a TIC use case and explains how federal agencies can apply and combine use cases to implement TIC security capabilities to secure their enterprises. The handbook should be used as a reference when implementing TIC use cases, in coordination with the TIC core guidance (see Figure 1).

This handbook does not prescribe which use cases federal agencies should reference, or combine, to secure their environment. Agencies are expected to assess their architecture to determine which use cases are applicable and to implement the appropriate security capabilities accordingly. Agencies are encouraged to construct their architectures by combining individual use cases, as needed.

3. Overview of TIC Use Cases

TIC use cases provide guidance on the secure implementation of platforms, services, and environments, and will be released on an individual basis. The guidance is derived from pilot programs and best practices from the public and private sectors. The purpose of each TIC use case is to identify the applicable security architectures, data flows, and policy enforcement points (PEPs) and to describe the implementation of the security capabilities in a given scenario.

Use cases outline which security capabilities, such as endpoint and user-based protections, must be in place for specific instances where traffic does not flow through a traditional TIC access point. Due to the complexity of business mission needs and emerging technologies that drive development of new use cases, the capabilities provided in use case guidance may be separate from an agency's existing network boundary solution provided by a Trusted Internet Connection Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS).

Use cases build upon the key concepts presented in the *TIC 3.0 Reference Architecture* (Reference Architecture) and provides implementation guidance for applicable security capabilities defined in the *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog). TIC use cases articulate:

- Network scenarios for TIC implementation,
- Security patterns commonly used within the federal civilian enterprise, and
- Technology-agnostic methods for securing current and emerging network models.

TIC use cases provide architecture solutions that can be used in support of agency modernization efforts, including:

- Planning – Scope, schedule, resources, risks, and assumptions;
- Acquisitions – Key requirements and market research;
- Implementation – Greenfield or migration of existing system;
- Architecture Design and Diagrams – Data flow, transport, key security, monitoring services and capabilities, and policy enforcement points (PEPs); and
- Technical Analysis – Critical questions that need to be answered, measurements, and metrics.

Agencies are encouraged to leverage the Security Capabilities Catalog and TIC overlays, in conjunction with their risk management plan, to implement TIC use cases. In order to keep up with the rapid pace of technology and threat evolution, TIC use cases will be reviewed and updated on a regular basis.

3.1 Use Case Structure

Use cases contain the following components:

- **Description**: Identifies the scope of the use case;
- **Assumptions and Constraints**: Outlines the assumptions and constraints about the trust zones and data flows in the use case;
- **Conceptual Architecture**: Describes the trust zones, policy enforcement points (PEPs), data flows, one or more security patterns, and optional implementations of a specific computing scenario (e.g., branch office, remote user, etc.);
- **TIC Security Capability Guidance**: Provides guidance to facilitate agency implementation of TIC security capabilities within the use case scenario; and
- **Telemetry Requirements**: Highlights when agencies must share telemetry with CISA.

3.2 Assumptions and Caveats

The following list of assumptions and caveats apply to all TIC use cases.

- Use cases are based on architectures that have been successfully piloted or otherwise implemented.
- Use cases are not intended to apply to every implementation of a given architecture (e.g., an email-as-a-service (EaaS) use case may not directly align with an agency's use of an EaaS solution).
- Use cases are vendor, agency, and technology-agnostic.
- Unless noted, each use case is independent of other use cases.
- Each use case will refer to a specific version of the Security Capabilities Catalog for traceability.

4. Use Case Creation and Management

CISA is responsible for creating use cases, and the Federal CISO Council TIC Subcommittee is responsible for their approval. CISA may produce use cases from agency pilots or implementations. CISA, in coordination with stakeholders, will update use cases over time to reflect changes in technology or feedback from agencies and service providers. The process for creating and managing use cases is depicted in Figure 2.

Figure 2: Use Case Creation Process

5. Use Case Implementation

Agencies have flexibility in implementing a TIC use case. The use cases are designed to provide a variety of implementation options and scenarios, so agencies can customize the implementation of TIC 3.0 guidance based on their architectures. While use cases are created based on pilots and implementations from various agencies, use cases can be uniquely applied across the .gov. The following sections describe the liberties agencies have for tailoring the use cases to their specific needs.

5.1 Connecting Use Cases

An agency may combine one or more use cases to best implement TIC 3.0 in its architecture. Agencies have the discretion to display the relationships and interpret the interactions between use cases to best suit their needs. For example, the relationship between two infrastructure-as-a-service (IaaS) use cases may be different than the relationship between an IaaS use case and a software-a-a-service (SaaS) use case. The implementation details for integrating the use cases will depend on the specific agency environment and are beyond the scope of the individual use case.

5.2 Choosing Security Patterns

Use cases may provide more than one option for implementing a security pattern in order to give agencies flexibility. Each security pattern may have its own implementation options. The use case may include associated capabilities or implementation guidance for the security patterns or the common options for implementing those security capabilities.

Figure 3 provides an example set of implementation options for a security pattern linking the web and a branch office. While the implementation options in a use case typically apply to the most common agency deployments, agencies may implement other options, based on their unique needs. Agencies are encouraged to explore the variety of security patterns typically included in TIC use cases.

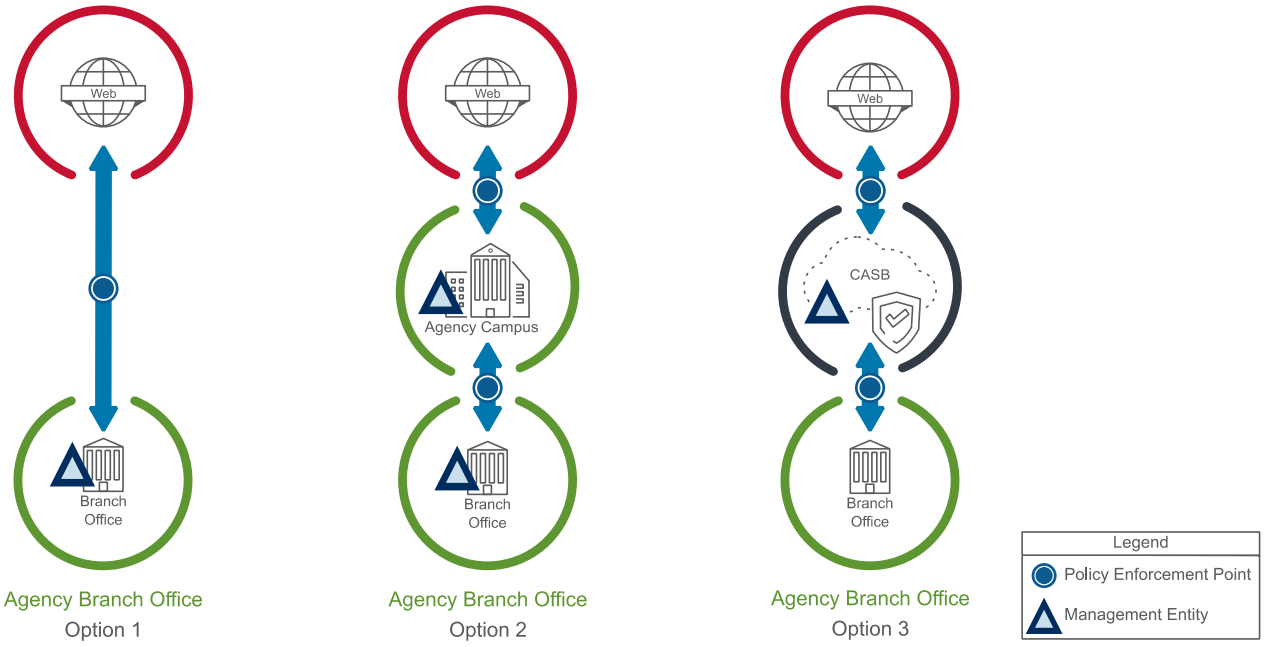

Figure 3: Example Security Pattern Implementation Options

5.3 Customizing Trust Zones

Each trust zone in a use case will be labeled with a high, medium, or low trust level, based on a pilot implementation or best practice. Agencies can modify this trust zone designation to meet their needs based on their risk tolerance and depending on their considerations for a specific scenario. For example, a use case might designate a cloud service provider (CSP) as medium trust zone, but an agency may consider a CSP to be a high trust zone based on unique circumstances, like stronger contractual terms that provide greater visibility into its CSP. Additional examples of how the same type of environment can have a different trust level designation are depicted in Figure 4.

Figure 4: Trust Level Designation Examples

Agencies can also nest trust zones within a larger, primary trust zone, as depicted in Figure 5. The nested trust zones share a boundary that is secured by the same PEP(s). In this example, the agency campus, branch office, remote user, and TIC access point are nested within a single trust zone where the data flowing in and out of the zones traverse the same PEP, which is the TIC access point in this case.

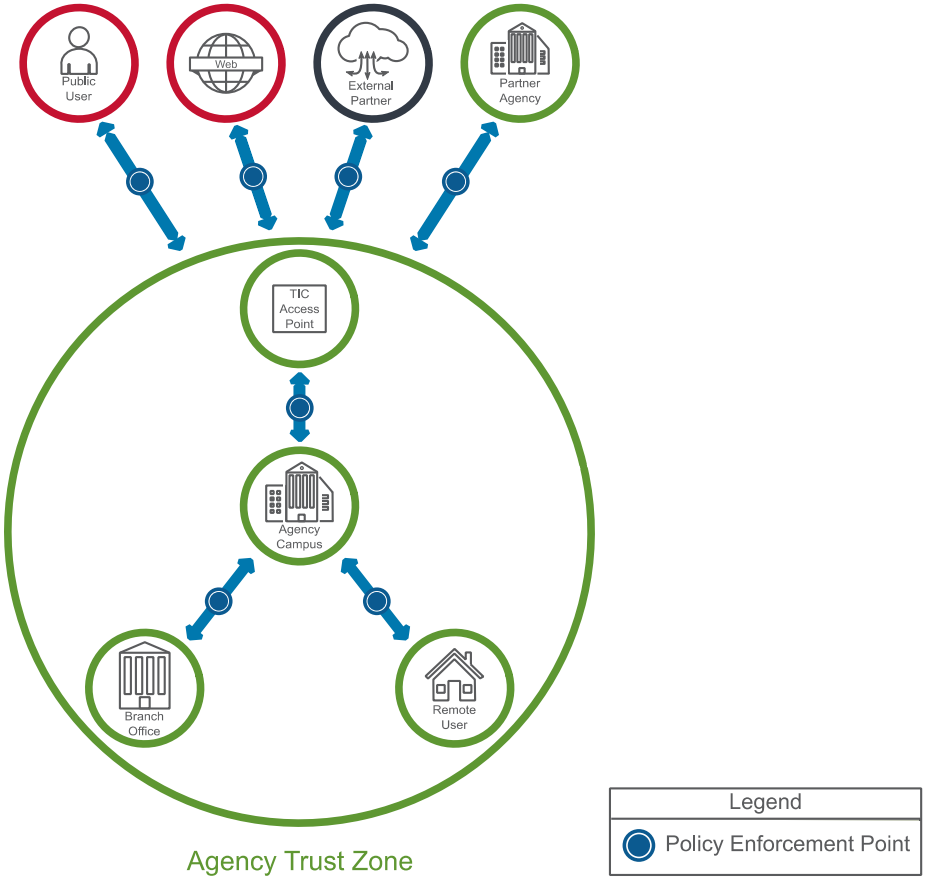

Figure 5: Example of Nested Trust Zones

It is important to note that the security pattern depicted in Figure 5 can be tailored depending on an agency's unique requirements. For example, while this nested representation includes the TIC access point, some traditional TIC deployments may have the TIC access point outside the Agency Trust Zone. Also, some agencies' deployments of the *TIC 3.0 Traditional TIC Use Case* (Traditional TIC Use Case) may include only a subset of the listed trust zones.

The Reference Architecture provides criteria and considerations to help facilitate decision-making for agencies when determining the appropriate level of trust within a given environment and the consequent level of rigor to employ when implementing security capabilities. Ultimately, the trust level designation for a zone should reflect its risk posture; agencies are responsible for implementing protections that are commensurate with the designated trust level of a zone and its security risks.

Refer to the Reference Architecture for more details on trust zones and trust levels.

5.4 Applying Security Capabilities and Rigor

When securing trust zones, agencies should consider unique data sensitivity criteria and the impact of compromise to agency data stored in trust zones. Agencies may apply additional security capabilities that

have not been included in the use case to reflect their risk tolerances, early adoption of security capabilities, maturity level of existing cyber programs, and other factors.

Agencies also have the discretion to determine the level of rigor necessary for applying security capabilities to use cases, based on federal guidelines and their risk tolerance. CISA recommends agencies use the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the NIST Special Publication (SP) 800-53, and other cybersecurity best practices and requirements to determine the appropriate security capabilities and level of rigor. Figure 6 depicts a high-level implementation of the TIC guidance to an agency's risk framework.

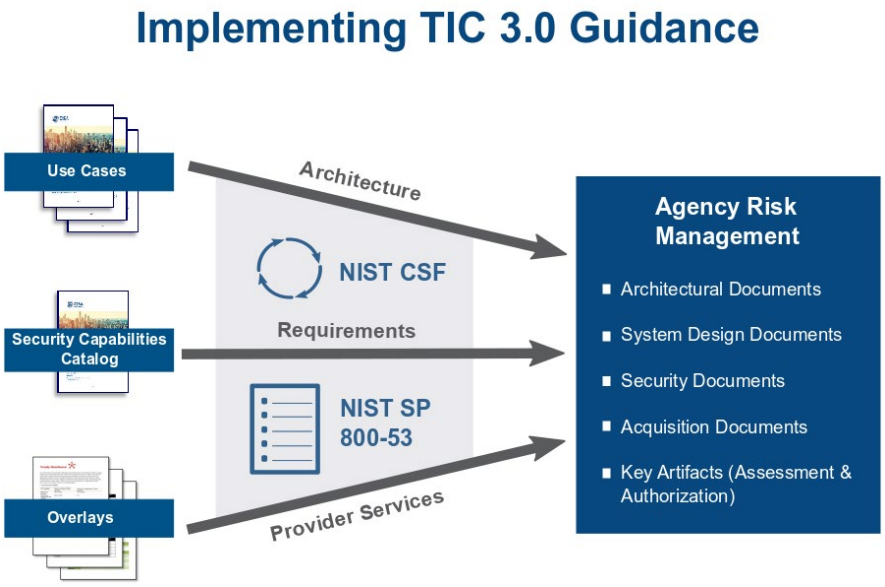

Figure 6: How an Agency Can Integrate TIC into its Risk Management Plan

6. Conclusion

The TIC 3.0 initiative provides federal agencies with greater flexibility in designing networks and acquiring new information technology solutions. The Use Case Handbook explains how agencies can utilize and combine TIC use cases to deploy and secure modern architectures, in accordance with OMB M-19-26. The handbook should be used as a reference when implementing TIC use cases, in coordination with the TIC 3.0 core guidance.

Appendix A – Glossary and Definitions

Boundary: A notional concept that describes the perimeter of a zone (e.g. mobile device services, general support system (GSS), Software-as-a-Service (SaaS), agency, etc.) within a network architecture. The bounded area must have an information technology (IT) utility.

Internet: The internet is discussed in two capacities throughout TIC documentation:

1. A means of data and IT traffic transport.
2. An environment used for web browsing purposes, referred to as "Web."

Managed Trusted Internet Protocol Services (MTIPS): Services under GSA's Enterprise Infrastructure Solutions (EIS) contract vehicle that provide TIC solutions to government clients as a managed security service. It is of note that the EIS contract is replacing the GSA Networx contract vehicle that is set to expire by Fiscal Year (FY) 2023.

Management Entity (MGMT): A notional concept of an entity that oversees and controls security capabilities. The entity can be an organization, network device, tool, service, or application. The entity can control the collection, processing, analysis, and display of information collected from the policy enforcement (PEPs), and it allows IT professionals to control devices on the network.

National Cyber Protection System (NCPS): An integrated system-of-systems that delivers a range of capabilities, including intrusion detection, analytics, intrusion prevention, and information sharing capabilities that defend the civilian Federal Government's information technology infrastructure from cyber threats. The NCPS capabilities, operationally known as EINSTEIN, are one of several tools and capabilities that assist in federal network defense.

Policy Enforcement Point (PEP): A security device, tool, function, or application that enforces security policies through technical capabilities.

Policy Enforcement Point Security Capabilities: Network-level capabilities that inform technical implementation for relevant use cases.

Reference Architecture (RA): An authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.

Risk Management: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Tolerance: The level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame. An organization's risk tolerance level is the amount of corporate data and systems that can be risked to an acceptable level.

Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals). Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

Security Pattern: Description of an end-to-end data flow between two trust zones. Security patterns may have an associated set of security capabilities or guidance to secure the data flow along with one or more of the zones.

Seeking Service Agency (SSA): An agency that obtains TIC services through an approved Multi-Service TICAP.

Security Information and Event Management (SIEM): An approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

Telemetry: Artifacts derived from security capabilities that provide visibility into security posture.

TIC: The term "TIC" is used throughout the Federal Government to denote different aspects of the TIC initiative; including the overall TIC program, a physical TIC access point (also known as a Traditional TIC), and a TIC Access Provider (TICAP – see below). This document refers to TIC as an adjective or as the Trusted Internet Connections initiative.

TIC Access Point: The physical location where a federal civilian agency consolidates its external connections and has security controls in place to secure and monitor the connections.

TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

TIC Initiative: Program established to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet. Key stakeholders include CISA, OMB, and GSA.

TIC Overlay: A mapping from products and services to TIC security capabilities.

TIC Use Case: Guidance on the secure implementation and/or configuration of specific platforms, services, and environments. A TIC use case contains a conceptual architecture, one or more security pattern options, security capability implementation guidance, and CISA telemetry guidance for a common agency computing scenario.

Trust Zone: A discrete computing environment designated for information processing, storage, and/or transmission that dictates the level of security necessary to protect the traffic transiting in and out of a zone and/or the information within the zone.

Unified Communications and Collaboration (UCC): A collection of solutions designed to facilitate communication and collaboration, including in real-time, such as required by remote work or collaboration between locations.

Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.

Web: An environment used for web browsing purposes. Also see Internet.

Zero Trust: A security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.