CISA
CYBER+INFRASTRUCTURE

Trusted Internet Connections 3.0

Vol. 4:

Use Case Handbook

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Draft

Document Status

This document is a draft and open for public comment. The Cybersecurity and Infrastructure Security Agency is requesting feedback and comments through January 31, 2020.
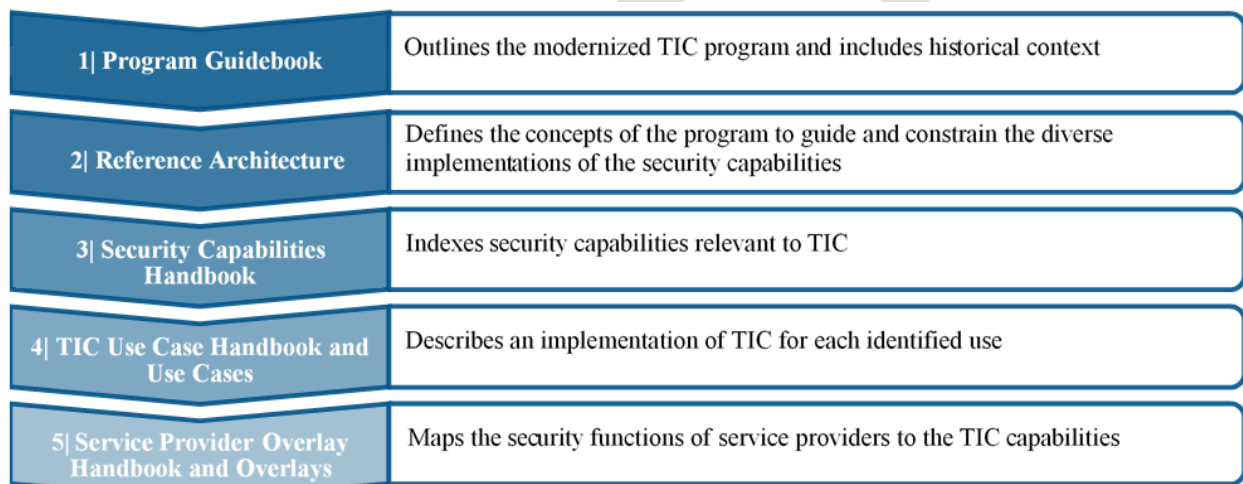
Disclaimer

The Trusted Internet Connections (TIC) 3.0 implementation guidance is described throughout a series of documents. Each document builds on the other and is referenced as sequential volumes. Readers should refer to the first volume, the TIC 3.0 Program Guidebook, as the principal guidance document.

Reader's Guide

The initiative is defined through key documents that describe the directive, the program, the capabilities, the implementation guidance, and a mapping to service providers. 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
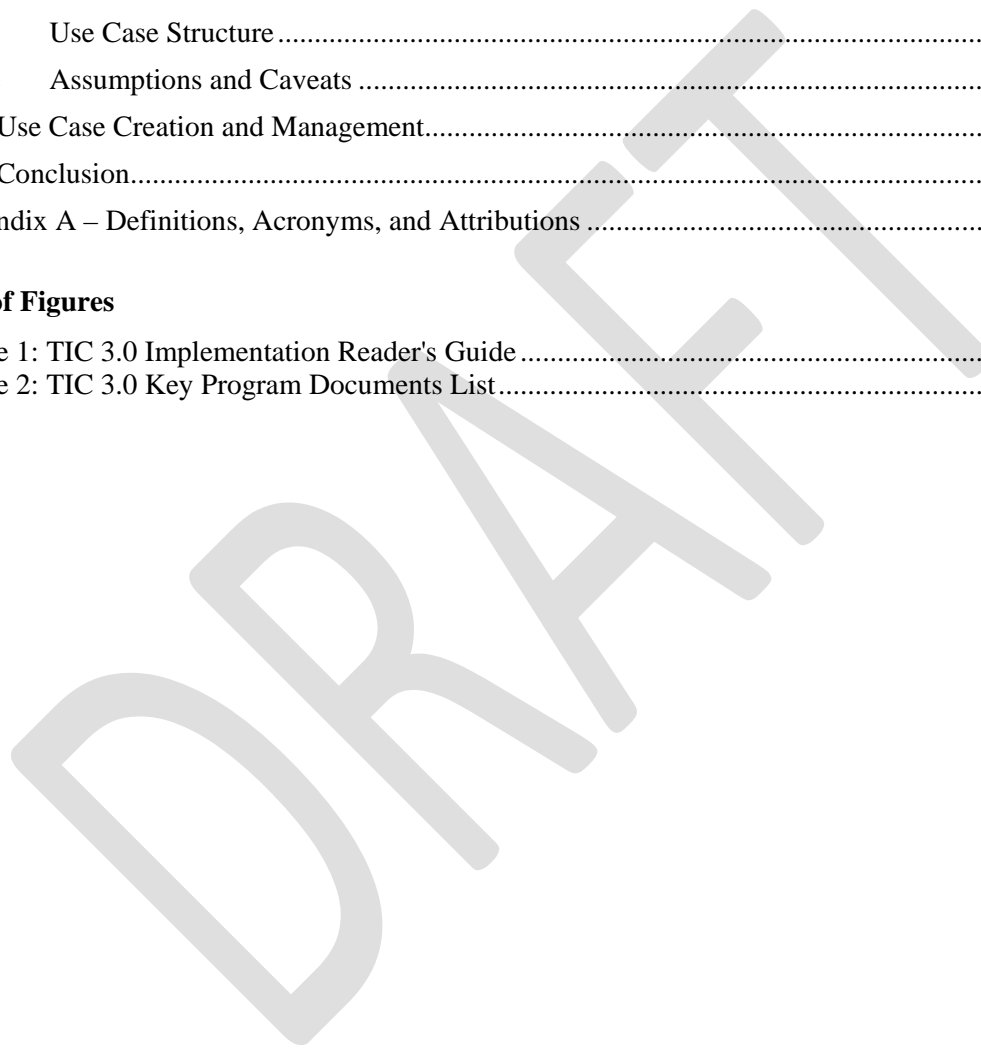
Figure 1: TIC 3.0 Implementation Reader's Guide

1| Program Guidebook	Outlines the modernized TIC program and includes historical context
2| Reference Architecture	Defines the concepts of the program to guide and constrain the diverse implementations of the security capabilities
3| Security Capabilities Handbook	Indexes security capabilities relevant to TIC
4| TIC Use Case Handbook and Use Cases	Describes an implementation of TIC for each identified use
5| Service Provider Overlay Handbook and Overlays	Maps the security functions of service providers to the TIC capabilities

TIC 3.0 Use Case Handbook

Table of Contents

List of Figures

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, setting requirements and an execution framework for agencies to implement a baseline perimeter security standard.

The initial versions of TIC consolidated federal networks and standardized 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 TIC expands upon the original program 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

In an effort 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.

Hybrid TIC Model: An alternative approach to implementing TIC services that blends the use of agency hosted and managed TIC access providers (TICAP) and MTIPS solutions.

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 close out by FY 2023.

Management Entity (MGMT): A notional concept of an entity that oversees and controls the protections for data. The entity can be an organization, network device, tool, function or application. The entity can control the collection, processing, analysis, and display of information collected from the 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: Used to articulate security best practices and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means (i.e., functionality in hardware,

---

[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 >.

software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

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

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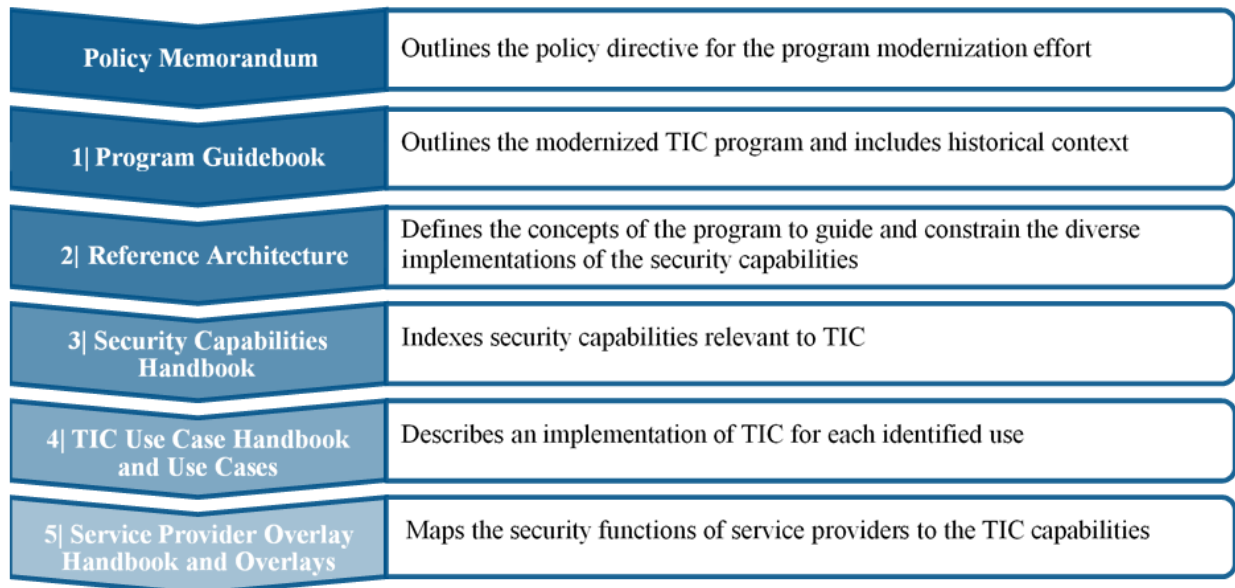
TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

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.

2. Purpose and Limitations

The use cases provide vendor-agnostic examples of TIC architectures and guidance on the secure implementation and/or configuration of applications, services, and environments. The TIC 3.0 Use Case Handbook begins to explain at an architectural level how federal agencies can utilize use cases to secure given computing scenarios in accordance with TIC requirements. The handbook should be used in collaboration with other TIC program documents (Figure 2) to achieve the program's goals.

Figure 2: TIC 3.0 Key Program Documents List

Policy Memorandum	Outlines the policy directive for the program modernization effort
1| Program Guidebook	Outlines the modernized TIC program and includes historical context
2| Reference Architecture	Defines the concepts of the program to guide and constrain the diverse implementations of the security capabilities
3| Security Capabilities Handbook	Indexes security capabilities relevant to TIC
4| TIC Use Case Handbook and Use Cases	Describes an implementation of TIC for each identified use
5| Service Provider Overlay Handbook and Overlays	Maps the security functions of service providers to the TIC capabilities

The handbook does not explain 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 implement the appropriate TIC capabilities accordingly. Individual use cases may lack the

architectural components present, or desired, in an agency's environment. Agencies are expected to combine use cases, as needed, to identify the security controls needed to protect their specific computing scenario.

3. Use Cases

TIC 3.0 use cases outline which alternative security controls, such as endpoint and user-based protections, must be in place for specific instances where traffic is not required to flow through a traditional TIC access point. The capabilities used to meet the use case guidance may be separate from an agency's existing network boundary solutions provided by a Trusted Internet Connection Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS). Agencies are expected to satisfy TIC use case capabilities to secure network boundaries, including instances when TICAP or MTIPS services are not utilized.

Use cases describe the current state challenges and limitations, characteristics, scope, and target state for a given computing scenario. They also provide agencies with an overall approach for planning, acquiring, and securely implementing technologies and services. Use cases are intended to be supported by other artifacts, like the TIC 3.0 Reference Architecture or the TIC 3.0 Security Capabilities Handbook. Individual use cases may be supported by multiple sets of supporting artifacts based on differing operational characteristics and development of capabilities provided by service providers.

3.1   Use Case Structure

Use cases typically contain the following components:

- **Description**: Identifies the scope of the use case;
- **Assumptions and Constraints**: Outlines the presumptions and limitations of the use case;
- **TIC Security Capability Guidance**: Provides contextual information to facilitate agency implementation of TIC capabilities;
- **Conceptual Architecture**: Displays a high-level visualization of a specific computing scenario (e.g., branch office, remote user, etc.); and
- **Security Patterns**: Represent the visualization of environments and policy enforcement points in a computing scenario.

3.2   Assumptions and Caveats

The use cases should only be considered with the following list of assumptions and caveats.

- Use cases are based on TIC implementations that have been successfully piloted or otherwise vetted by CISA (e.g., through pilot lessons learned).
- An agency may combine one or more use cases to satisfy TIC requirements.
- Use cases are not intended to apply to every agency implementation of a given architecture type (e.g., the 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.

4. Use Case Creation and Management

CISA is responsible for creating use cases and the Federal Chief Information Security Officer Council TIC Subcommittee is responsible for their approval. CISA may produce use cases from agency pilots or

generate them independently. CISA will update use cases over time to reflect changes in technology or agency/service provider feedback.

5. 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 use cases to secure their architectures and comply with TIC requirements. The proper implementation of TIC promotes secure network and perimeter traffic within the federal enterprise trust zones and expands into all agency traffic. Agencies are expected to secure network boundaries in accordance with OMB Memorandum M-19-26.

Appendix A – Definitions, Acronyms, and Attributions

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.

Cloud Services: Cloud services are a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Control: The amount of authority an agency has over an environment's security policies, procedures and practices.

Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Hybrid TIC Model: An alternative approach to implementing TIC services that blends the use of agency hosted and managed TIC access providers (TICAP) and MTIPS solutions.

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"

Logical Architecture: A structural design that gives an appropriate level and as much detail as possible without constraining the architecture to a particular technology or environment.

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 close out by FY 2023.

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

National Cyber Protection System (NCPS): A system responsible for cyber activity analysis and response that works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets.

Personal Devices: Devices owned by an employee that is used for work purposes and/or contains the employer's data.

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

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: Used to satisfy the security requirements and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and 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).

Trust Zone Diagram: A diagram used to connect the concepts of TIC 3.0—designate trust zones and identify the locations of the PEPs and the MGMT—over a logical architecture

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

Sensitivity: The impact of compromise to an information system's confidentiality, integrity or availability.

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.

Software-as-a-Service (SaaS): A software distribution model in which a third-party provider hosts an application and makes it available to customers over the internet.

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 manage and host 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: Presidential directive to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet.

TIC Use Case: A document that identifies the applicable security capabilities and describes the implementation of the capabilities in a given scenario.

Transparency: The degree of visibility an agency has into an environment.

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.

Verification: The extent to which an agency can verify an environment's compliance with relevant controls, standards and best practices.

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.

Zone: A portion of a network that has specific security requirements.