CISA
CYBER+INFRASTRUCTURE

Trusted Internet Connections 3.0

Vol. 5:
Service Provider Overlay Handbook

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

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.

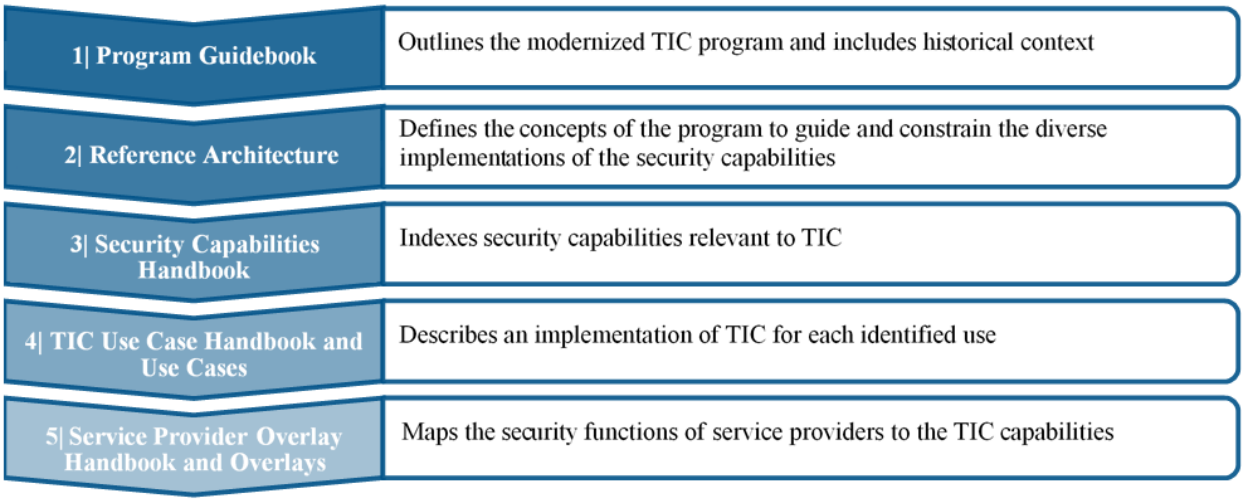
Disclaimer

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



TIC 3.0 Service Provider Overlay 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, 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.

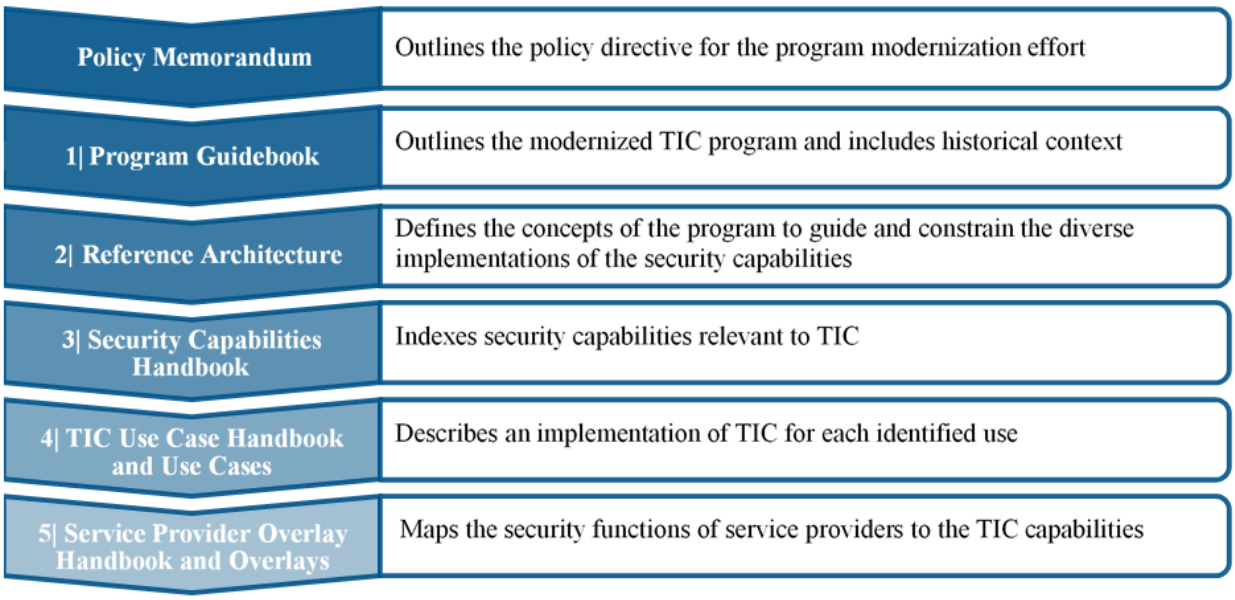
TIC Access Provider (TICAP): An agency or vendor that manages and hosts one or more TIC access points. Single Service TICAPs serve as a TIC Access Provider only to their own agency. Multi-Service TICAPs also provide TIC services to other agencies through a shared services model.

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 Service Provider (SP) Overlays map TIC security capabilities to security solutions available through specific cloud vendors. The SP Overlay Handbook describes ways that federal agencies can utilize SP Overlays to secure their cloud environments in accordance with TIC guidance. 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



The handbook does not describe which security services federal agencies should select or provide configuration guidance. Agencies are expected to use risk management practices to select the security capabilities appropriate for their unique environments and risk tolerances. Agencies are also expected to

work closely with service providers to ensure security capabilities are properly configured and maintained.

3. Service Provider Overlays

SP Overlays accelerate cloud adoption by identifying the TIC-compatible security solutions agencies can select from service providers, or vendors, to assist in protecting their cloud environments. An overlay should be considered as a high-level mapping of a vendor's services against the security capabilities and appliances in a traditional service environment. Some vendor solutions may not align with TIC security capabilities, and agencies may need to obtain additional security services from other third-party providers to secure their environments.

The overlays should be considered independent of the TIC Use Cases. While the overlays can be used in tandem with the use cases, an overlay is not mapped to any specific TIC Use Case. An agency may couple an overlay with multiple use cases, or an agency may try to apply multiple overlays with a use case.

3.1 Service Provider Overlay Structure

Each overlay contains three columns:

TIC Security Capability: The security capability, derived from the TIC security objectives described in the TIC 3.0 Security Capabilities Handbook, is 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). The capabilities shown will only be a subset of a growing set of security capabilities.

Traditional On-Premise TIC Access Point: The appliances and services that are typically hosted in a traditional TIC access point, that is on-premises (on-prem), include services that are used to manage and monitor the TIC access point.

Service Provider Security Solution: The vendor-supplied security solution that is expected to map to a specific TIC security capability.

Table 1: Notional TIC 3.0 SP Overlay

TIC Security Capability	Traditional On-Prem TIC Access Point	CSP Security Solution
Stateful or Stateless Access Lists	Firewall	Name of Vendor Solution
Break and Inspect		Name of Vendor Solution
IDS/IPS		
VPN	VPN Concentrator	3rd Party Only
Event and Incident Correlation	SIEM	Name of Vendor Solution
		Name of Vendor Solution

3.2 Assumptions and Caveats

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

- Overlays are intended to provide a high-level mapping of vendor services.
- Overlays do not make assertions regarding the strength of the mappings.

- Overlays do not assert the quality of a vendor's services.
- Overlays should be considered independent of the TIC Use Cases.
- Overlays do not offer awareness on the configuration or implementation that is required.
- Vendor services tend to overlap, or may be more granular than, in a traditional TIC environment.
- The SP may have a gap in a particular capability, which will be reflected in the overlay as a "3rd Party Service."
- Mappings may be imprecise as it can be difficult to map each vendor's security solution to a specific TIC security capability.
- Agencies are expected to work with vendors to obtain detailed information about their cloud security solutions.
- Overlay formats may need to be adjusted to support PaaS and SaaS solutions.

4. Overlay Creation and Management

The CISA TIC program management office (PMO) will collaborate with service providers to develop SP Overlays. The overlays are independent of the TIC Use Cases, and the TIC PMO may work directly with service providers to create overlays. The TIC PMO will use data from the *Federal Information Security Management Act of 2014 (FISMA 2014)*[2], as well as suggestions from the Federal Chief Information Security Officers Council TIC Subcommittee and TIC working groups, to determine which service providers to work with to develop an overlay.

Recognizing that vendor services may change or be rebranded, the TIC PMO will periodically refresh the overlays as applicable. Unless there is a specific circumstance, it is not expected that a service provider's overlay will be updated more than once a year.

The TIC PMO may not agree with every vendor's service mapping to a TIC capability. In instances when the service provider and the TIC PMO do not agree on a mapping, the TIC PMO will not include the mapping in the overlay.

5. Conclusion

The TIC 3.0 initiative provides federal agencies with greater flexibility in designing networks and acquiring new information technology solutions. The Service Provider Overlay Handbook explains how agencies can use overlays to select security capabilities furnished by service providers. Agencies are expected to configure services in accordance with OMB Memorandum M-19-26. The proper implementation of TIC promotes secure network traffic within the federal enterprise trust zones and expands into all agency traffic, including cloud communications.

[1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

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.