# Trusted Internet Connections 3.0

## TIC Core Guidance Volume 5:

## Overlay 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.

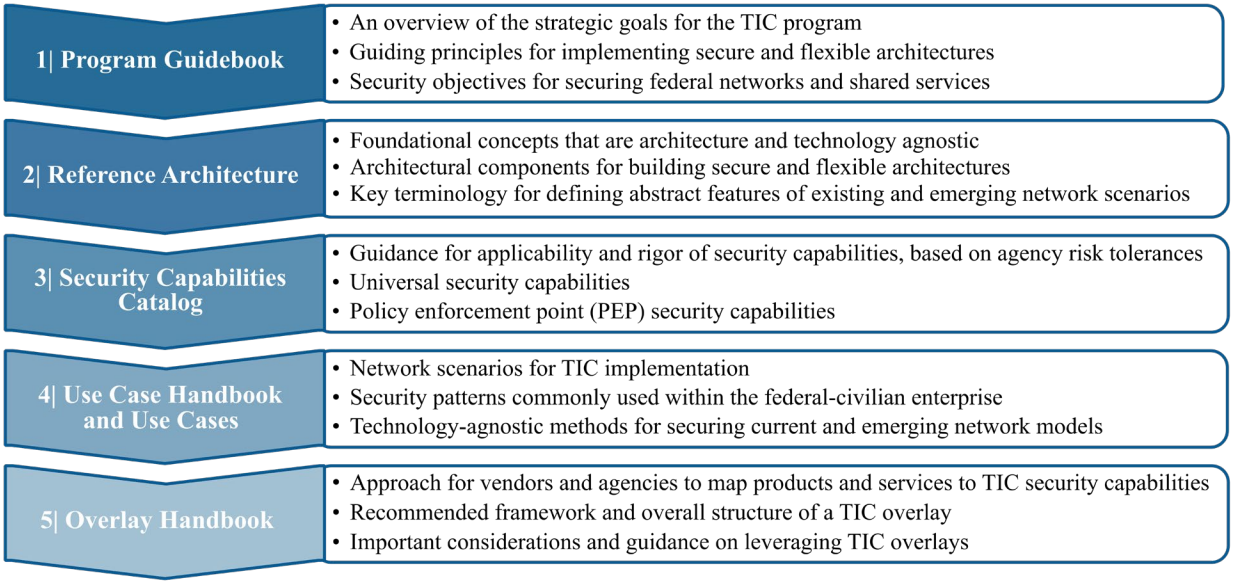



*Figure 1: TIC 3.0 Guidance Snapshot*

# TIC 3.0 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 boundary 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 boundary 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 in 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 Overlay Handbook

The *TIC 3.0 Overlay Handbook* (Overlay Handbook) guides vendors on how to create overlays that map products and services to TIC security capabilities. The Overlay Handbook can also be used by agencies, alongside TIC overlays, to assess the capabilities of vendors when making decisions on the procurement of products and services. The handbook should be used in collaboration with other TIC program documents (see Figure 1) to achieve the program's goals.

The handbook does not direct agencies to select specific security services nor does it provide configuration guidance. Agencies are expected to use relevant TIC use cases, risk management artifacts, and best practices to select the security capabilities and implementations appropriate for their unique environments and risk tolerances. Agencies are also encouraged to work with vendors to ensure security capabilities are properly configured and maintained.

# 3. Overview of TIC Overlays

TIC overlays are intended to align TIC security capabilities, described in the *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog), with available vendor products, services, and applications. Overlays can facilitate cloud adoption by identifying TIC-compatible security solutions for cloud-based systems and services. However, overlays may not represent a comprehensive list of vendor services, and agencies are not constrained to solutions detailed in existing TIC overlays.

Overlays are created and managed by vendors. Overlays will most often be developed independently of TIC use cases. However, some overlays may be aligned to specific use cases in unique situations.

When implementing TIC use cases, agencies need to select security capabilities and the associated rigor of those capabilities in accordance with their security objectives and mission needs. Overlays are designed to help agencies select solutions to fulfill all, or only some, of the security capabilities they need.

An agency may use a single overlay to inform the implementation of one or more use cases. Conversely, an agency may use multiple overlays, when combining services of more than one vendor, to inform the implementation of a single use case. Agencies have the flexibility to select vendor solutions and augment these solutions to make them compatible with their risk tolerance.

Agencies can use overlays to support the following activities:

- Planning – Scope, schedule, resources, risks, assumptions;
- Acquisitions – Key requirements, market research;
- Implementation – Greenfield or migration of existing systems;
- 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, measurement, and metrics.

Agencies may use overlays in conjunction with other artifacts to implement their TIC solutions.

- TIC 3.0 core guidance documentation
- TIC use cases
- Project plans
- Requirement plans
- Capability documentation
- Technical diagrams
- Security guidance and control tables
- Requirements traceability matrices

## 3.1 Overlay Structure

Each overlay is comprised of a series of tables that map TIC security capabilities to available products and services. Each table corresponds to either the universal security capabilities or a group of PEP security capabilities from the Security Capabilities Catalog. Each table should contain the five columns described below.

**TIC Security Capability:** Security capabilities, derived from the TIC 3.0 security objectives described in the *TIC 3.0 Program Guidebook* and other TIC 3.0 guidance, are combinations of mutually-reinforcing security controls (i.e., safeguards and countermeasures) which can be 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). Refer to the latest version of the Security Capabilities Catalog for the current list of TIC security capabilities.

**Primary Service(s):** This column names the products or services that directly fulfill specific TIC security capabilities. The column can be left blank if a vendor's services do not completely fulfill a security capability. Alternatively, if a vendor's services complement another vendor's service in fulfillment of the security capability, the authoring vendor may indicate the name of the other vendor and service in this column. If it is preferable for the other vendor to be unspecified, the authoring vendor can indicate the service generically as a third-party service.

**Complementary Service(s):** This column names the products or services that support, or partially fulfill, specific TIC security capabilities. Vendors may include services that provide enhancements to the services listed as primary services. Complementary services may also include services that, while not directly fulfilling a security capability, indirectly facilitate its fulfillment (e.g., providing an interface to a third-party solution). An authoring vendor may elect to include complementary services from a partnering vendor in this column as well.

**Service Description:** This is a brief description of the service(s) provided by the vendor. A link to the service description is a desired and acceptable entry for this field. Service descriptions should clarify the role and nature of security that the service provides. This column is optional and may be left blank.

**Configuration Guidance:** This is a brief description of the administration and configuration of the product(s) or service(s) which support each of the TIC security capabilities. A link to the configuration

description is a desired and acceptable entry for this field. Configuration guidance, if provided, should adequately describe the implementation of the service with respect to the applicable security capability. If possible, configuration guidance should include critical settings and the location of the PEP(s) (i.e., cloud-based, on-premises, on the endpoint, etc.).

These fields are depicted in the notional overlay mapping in Table 2. The mapping provides multiple scenarios that a vendor may encounter when developing its own TIC overlay. The notional overlay mapping in Table 2 is written with a fictitious vendor, "Vendor X," as the author. It showcases six fictional solutions ("Solution A" - "Solution E") offered by "Vendor X" that fulfill or partially fulfill the security capabilities. Example links to the description and configuration guidance for each of the solutions offered by "Vendor X" are included in the notional overlay mapping. Table 2 also includes references to another named vendor, "Vendor Y," and an anonymous vendor, "Third Party Service," to demonstrate how other vendor services can be depicted in an overlay.

*Table 2: Notional TIC 3.0 Overlay Mapping*

**Vendor X Service Mapping**

| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #1** | Solution A | - | http://example.com/SolutionA | http://example.com/SolutionA/configuration |
| **Security Capability #2** | - | - | - | - |
| **Security Capability #3** | Vendor Y Solution | Solution B | http://example.com/SolutionB | http://example.com/SolutionB/configuration |
| **Security Capability #4** | - | Solution C | http://example.com/SolutionC | http://example.com/SolutionC/configuration |
| **Security Capability #5** | Third-Party Service | Solution D | http://example.com/SolutionD | http://example.com/SolutionD/configuration |
| **Security Capability #6** | Solution E | Solution F | http://example.com/SolutionE<br>http://example.com/SolutionF | http://example.com/SolutionE/configuration<br>http://example.com/SolutionF/configuration |

A vendor can customize an overlay by providing additional details regarding the fulfillment of the TIC security objectives with specific vendor products and services. For example, some vendors may include any architecture diagrams that illustrate how their products are deployed.

The security capabilities will evolve over time, as will vendor products and services. Therefore, each TIC overlay should contain version details that help to align TIC documentation and vendor products and services in an overlay. It is critical that the overlay references the version of the Security Capabilities Catalog used in the mapping.

CISA recommends each overlay lists the following version details:

- Vendor or service provider name;
- Product or service version;
- Vendor platform name;
- Security Capabilities Catalog version;
- Publication date; and
- Revision history.

## 3.2 Assumptions and Caveats

The following list of assumptions and caveats apply to TIC overlays.

- Overlays are intended to provide a high-level mapping of vendor services.
- Overlays do not make assertions about the strength of the mappings, where some services may align almost completely with a security capability while other services may map more weakly.
- Overlays do not assert the quality or effectiveness of a vendor's services.
- Overlays are typically developed independently of TIC use cases.
- Overlays do not offer awareness of the configuration or implementation that is required.
- Vendor services tend to overlap, or may be more granular than, in a traditional TIC environment.
- A vendor may have a gap for a capability, which will be reflected in the overlay as either a third-party service or no mapping for that security capability.
- Mappings may be imprecise as it can be difficult to map each vendor's security solution to a specific TIC security capability.
- Agencies are encouraged to work with vendors to obtain information about their solutions.
- Overlay formats may need to be adjusted to support PaaS and SaaS solutions.

# 4. Overlay Creation and Management

The creation and management of TIC overlays are at the discretion of vendors. Vendors may invite agencies to collaborate in the overlay development process. Vendors and service providers may also submit overlays and updates to CISA for awareness. However, CISA does not approve, adjudicate, nor vet TIC overlays. CISA does not attest to the strength of vendor service mappings to the TIC security capabilities. Any feedback given by CISA should be considered as suggestions or considerations.

Recognizing that vendor services may change, new services may be released, and that the Security Capabilities Catalog may be updated, service providers are encouraged to periodically refresh their overlays to align with these changes. Refreshes should be performed on an as-needed basis, but there is no requirement that overlays must be refreshed at a certain time interval if they remain applicable.

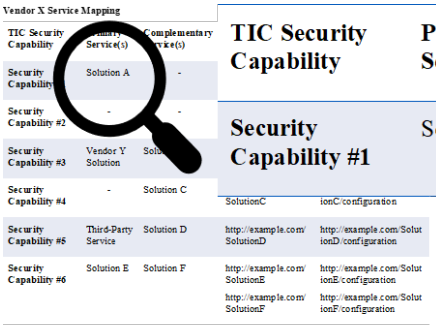
## 4.1 Creation Guidance by Scenario

To encourage consistency between TIC overlays and for ease of use by agencies, CISA recommends that overlays follow a similar format using the notional mapping depicted in Table 2 and the list of TIC security capabilities found in the latest Security Capabilities Catalog. Vendors should also refer to Section 3.1 above to understand the meaning of each column in an overlay table when creating an overlay to ensure consistency. Templates and additional guidance on overlays may be obtained by contacting CISA. Contact information can be found on CISA's TIC web page, www.cisa.gov/trusted-internet-connections.

To further assist vendors in developing TIC overlays, directions for completing an overlay mapping is outlined by common scenarios. The scenarios leverage the example overlay mapping for a fictitious vendor ("Vendor X") in Table 2.

### 4.1.1 Vendor Service(s) Fulfill a TIC Capability

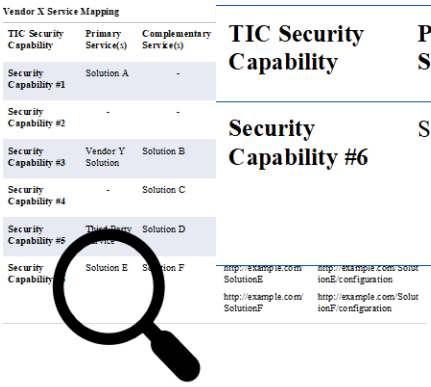
In this scenario, the vendor ("Vendor X") determines that one or more of its products and services directly fulfills a specific TIC capability. As shown in Figure 2, the vendor will input this product or service ("Solution A") into an overlay mapping table as a primary service. In this example, the vendor does not have any products or services that complement the primary service in fulfillment of the specified TIC capability, so the corresponding cell is left blank. The service description and configuration guidance for the fictitious service are inputted into the table as fictitious links to the vendor website.




| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #1** | Solution A | - | http://example.com/SolutionA | http://example.com/SolutionA/configuration |

*Figure 2: Vendor X Service is a Primary Service*

Similar to the previous example, Figure 3 depicts a scenario in which the vendor ("Vendor X") determines that one or more of its products and services directly fulfills a specific TIC capability and another product or service complements or enhances the main service. In this example, the vendor will input the product or service ("Solution E") that directly fulfills the respective capability as a primary service and input the product or service ("Solution F"), that enhances the main service, as a complementary service. The service description and configuration guidance for the fictitious services are inputted into the table as fictitious links to the vendor website.

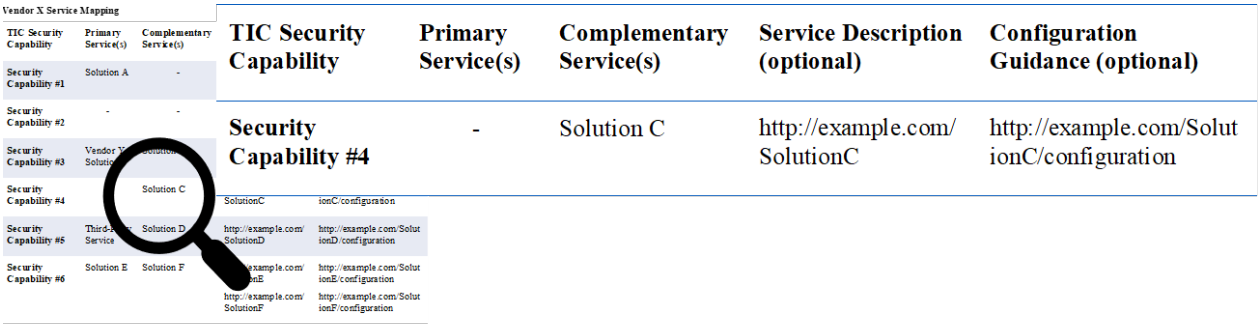



| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #6** | Solution E | Solution F | http://example.com/SolutionE<br>http://example.com/SolutionF | http://example.com/SolutionE/configuration<br>http://example.com/SolutionF/configuration |

*Figure 3: Vendor X Services are Primary and Complementary Services*

### 4.1.2 Vendor Service(s) Partially Fulfill a TIC Capability

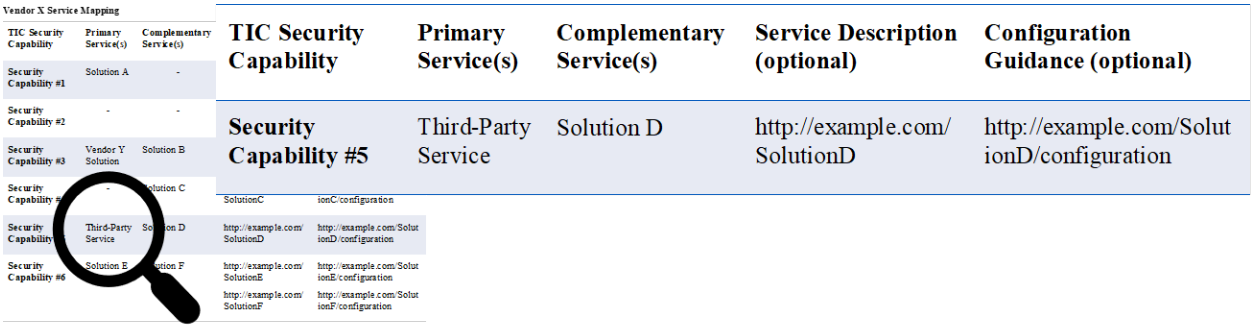
In this scenario, the vendor ("Vendor X") determines that one or more of its products and services supports, or partially fulfills, a specific TIC capability. As shown in Figure 4, the vendor will input this product or service ("Solution C") into an overlay mapping table as a complementary service. In this example, the vendor does not have any services that completely fulfills the specified TIC capability, so the corresponding cell for the primary service is left blank. The service description and configuration guidance for the fictitious service are inputted into the table as fictitious links to the vendor website.



| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #4** | - | Solution C | http://example.com/SolutionC | http://example.com/SolutionC/configuration |

*Figure 4: Vendor X Service is a Complementary Service*

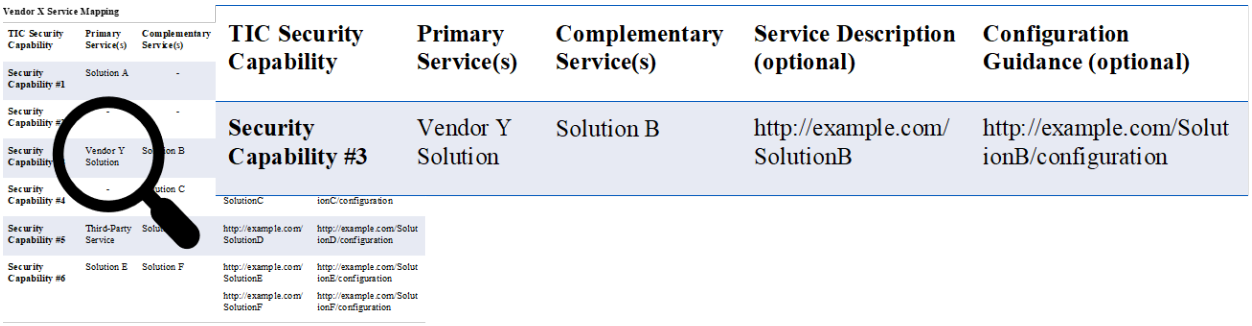
This scenario also includes two situations: 1) when the vendor ("Vendor X") has services that provide enhancements to another vendor's services that directly fulfill a specific capability and 2) when the vendor services, while not directly fulfilling a security capability, indirectly facilitate its fulfillment, like providing an interface to a third-party solution. In this case, depicted in Figure 5, the vendor authoring the overlay will input its supporting service ("Service D") as a complementary service and indicate the third-party service ("Third-Party Service") as the primary service. The service description and configuration guidance for the fictitious service are inputted into the table as fictitious links to the vendor website.



| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #5** | Third-Party Service | Solution D | http://example.com/SolutionD | http://example.com/SolutionD/configuration |

*Figure 5: Vendor X Service Complements a Third-Party Service*

Similar to Figure 5, the vendor ("Vendor X") developing the overlay may choose to name the other vendor. In this case, depicted in Figure 6, the vendor will input the name of the other vendor and the respective service ("Vendor Y Solution") as the primary service rather than denoting a generic third-party service ("Third-Party Service"). The vendor will complete the remainder of the table in the same way as the previous scenario.

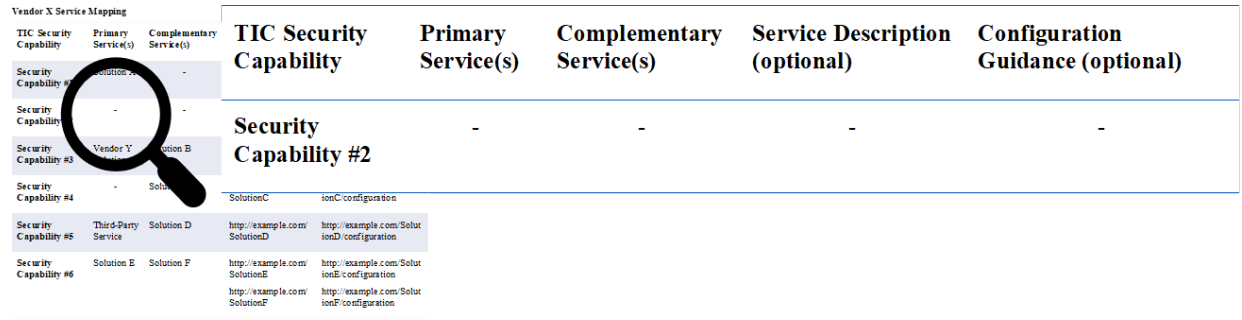


| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #3** | Vendor Y Solution | Solution B | http://example.com/SolutionB | http://example.com/SolutionB/configuration |

*Figure 6: Vendor X Service Complements Vendor Y Service*

### 4.1.3 Vendor Service(s) Do Not Fulfill or Support a TIC Capability

Vendors are encouraged to map all security capabilities identified in the most current version of the Security Capabilities Catalog to their services, even if a service does not align to a capability. In the case when the vendor ("Vendor X") does not have a service or product that fulfills or partially fulfills a security capability, the vendor will leave the row blank or indicate not applicable or no alignment. This example is depicted in Figure 7.



| TIC Security Capability | Primary Service(s) | Complementary Service(s) | Service Description (optional) | Configuration Guidance (optional) |
|---|---|---|---|---|
| **Security Capability #2** | - | - | - | - |

*Figure 7: Vendor X Services Do Not Align*

# 5. Overlay Implementation

Overlays help agencies expedite the implementation of the TIC use cases by providing a mapping between the TIC security capabilities and compatible industry solutions. While CISA does not attest to the strength of the mapping, it reduces the workload on agencies to research and identify potential solutions. Agencies should leverage the GSA Enterprise Infrastructure Solutions (EIS)[3] acquisition vehicle when procuring vendor services listed in the TIC overlays.

[3] "Enterprise Infrastructure Solutions," General Services Administration, https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions.

As illustrated in Figure 8, overlays are designed to be used with the other TIC 3.0 guidance to implement a TIC 3.0 architecture.

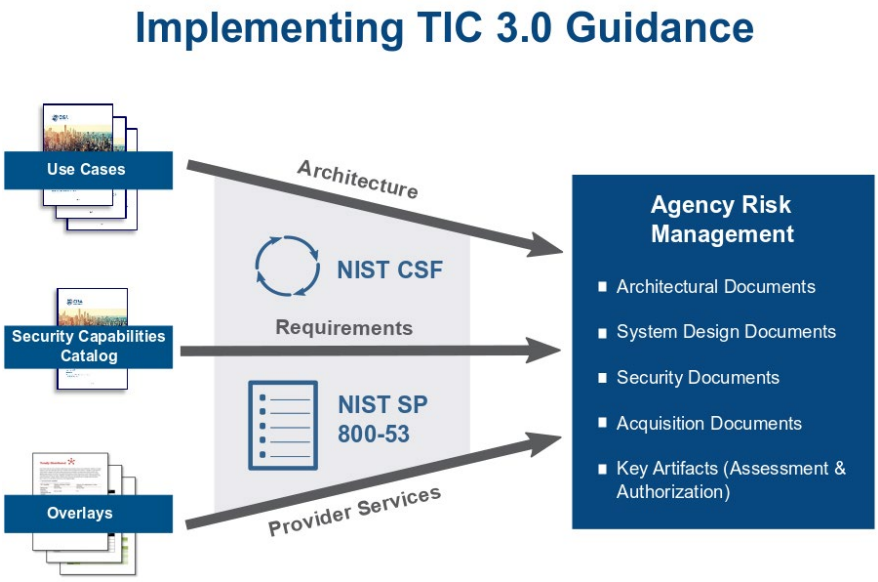



*Figure 8: How an Agency Can Integrate TIC into its Risk Management Plan*

When leveraging TIC overlays, agencies must recognize that a direct one-to-one mapping of vendor services to TIC security capabilities will not always be possible. A vendor service may align or partially align with more than one security capability, in which case an agency is free to use that service to help satisfy all applicable security capabilities. Similarly, individual vendor services may only partially align with a particular security capability or lack coverage for that capability. As such, satisfying a security capability may require the integration of multiple services, and agencies may need to obtain additional security services from other third-party providers to secure their environments.

To support agency risk management responsibilities, agencies should follow the GSA FedRAMP process and determine if any proposed cloud-based security solutions are authorized[4]. In the event, a cloud-based security solution is not yet FedRAMP authorized or in the process of obtaining authorization, agencies are responsible for assessment and authorization.

# 6. Conclusion

The TIC 3.0 initiative provides federal agencies with greater flexibility in designing networks and acquiring new information technology solutions. The Overlay Handbook explains how vendors can develop overlays and how agencies can use these overlays to select and tailor security capabilities furnished by service providers. Agencies should consult the overlays to implement TIC security capabilities that meet their business and risk management needs.

[4] "FedRAMP Marketplace," General Services Administration, https://marketplace.fedramp.gov/#!/products?sort=productName.

# 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 in 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.