Trusted Internet Connections 3.0

Traditional TIC Use Case

April 2021

Version 1.0

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.

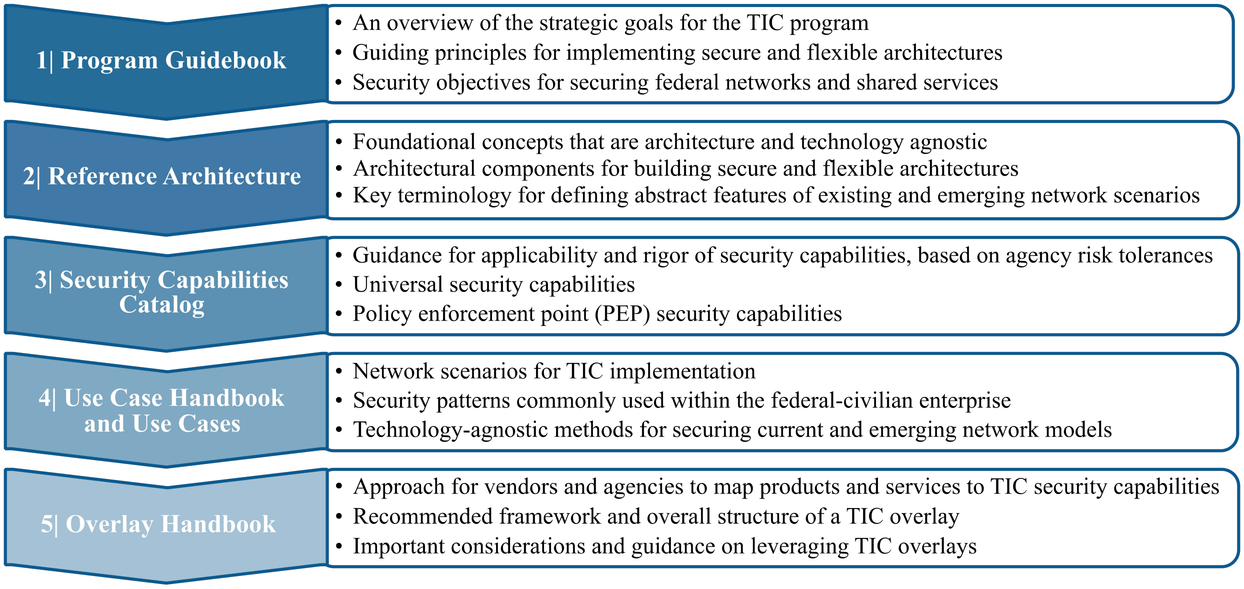
Table 1: Revision History

Version	Date	Revision Description	Section/Pages Affected
Draft	December 2019	Initial Release	All
1.0	April 2021	Response to RFC and Stakeholder Feedback	All

This use case references *Trusted Internet Connections 3.0 Security Capabilities Catalog* v1.1, dated April 2021. The applicable security capabilities will be further explained in the document.

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 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.



1| Program Guidebook

- An overview of the strategic goals for the TIC program
- Guiding principles for implementing secure and flexible architectures
- Security objectives for securing federal networks and shared services

2| Reference Architecture

- Foundational concepts that are architecture and technology agnostic
- Architectural components for building secure and flexible architectures
- Key terminology for defining abstract features of existing and emerging network scenarios

3| Security Capabilities Catalog

- Guidance for applicability and rigor of security capabilities, based on agency risk tolerances
- Universal security capabilities
- Policy enforcement point (PEP) security capabilities

4| Use Case Handbook and Use Cases

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

5| Overlay Handbook

- Approach for vendors and agencies to map products and services to TIC security capabilities
- Recommended framework and overall structure of a TIC overlay
- Important considerations and guidance on leveraging TIC overlays

Figure 1: TIC 3.0 Guidance Snapshot

TIC 3.0 Traditional TIC Use Case

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 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 R5)," September 2020. http://dx.doi.org/10.6028/NIST.SP.800-53r5.

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. Overview of TIC Use Cases

TIC use cases provide guidance on the secure implementation and configuration of specific 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. 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 build upon the key concepts and conceptual implementation of TIC 3.0 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). The *TIC 3.0 Use Case Handbook* (Use Case Handbook) provides general guidance for how agencies can use and combine use cases.

Agencies have flexibility in implementing TIC use cases. In particular:

- An agency may combine one or more use cases to best design and implement their TIC architectures.
- Use cases may provide more than one option for implementing a security pattern in order to give agencies flexibility.

- 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. The use cases are depicted following the schema illustrated in Figure 2. Agencies can modify this trust zone designation to meet their needs. Refer to the Reference Architecture for more details on trust zones.

High
Trust Zone
Medium
Trust Zone
Low
Trust Zone

Figure 2: Use Case Trust Zone Legend

- 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.
- Agencies have the discretion to determine the level of rigor necessary for applying security capabilities in use cases, based on federal guidelines and their risk tolerance.

Refer to the Use Case Handbook for more information on TIC use cases.

3. Purpose of the Traditional TIC Use Case

The TIC 3.0 Traditional TIC Use Case (Traditional TIC Use Case) defines how network security can be applied when an agency routes traffic from an agency campus to the web, trusted external partners, or partner government agencies through a traditional TIC access point, either an agency TIC Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS) provider. A trusted external partner may include an agency-sanctioned cloud service provider (CSP), or business partners, among others.

This use case includes four network security patterns:

- Secure agency campus access to web;
- Public user to secure agency campus;
- Secure agency campus access to agency-sanctioned external partners; and
- Secure agency campus access to partner agencies.

An agency may implement a subset of these traffic flows rather than all. For instance, an agency may not have trusted external partners.

The Traditional TIC Use Case is the "default use case." This use case demonstrates how TIC 2.2 security capabilities at a TIC access point can be used to implement TIC 3.0 to meet an agency's specific requirements, risk tolerances, and other factors.

OMB M-19-26 defines the Traditional TIC Use Case as the "default use case" which leverages agency TICAP and MTIPS providers. The Traditional TIC Use Case is intended to provide additional guidance to agencies and providers for how existing TIC 2.2 security capabilities at a TIC access point can be used to implement TIC 3.0 capabilities. While the TIC 2.2 security capabilities are consistent with the TIC 3.0 objectives, agencies may supplement the existing TIC 2.2 security capabilities with new TIC 3.0 security capabilities to reflect their agency requirements, risk tolerances, and other factors.

4. Assumptions and Constraints

This section outlines guiding assumptions and constraints for the Traditional TIC Use Case. It is intended to clarify significant details about the construction and replication of this use case.

The assumptions are broken down by the use case as a whole and by the unique entities discussed in the use case:

- Agency campus,
- TIC access point,
- External partners,
- Partner agencies,
- Web, and
- Public users.

The following are the assumptions and constraints of this use case.

- Requirements for information sharing with CISA in support of National Cyber Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) purposes are beyond the scope of this document. Consult the NCPS program[3] and CDM program[4] for further details.
- The TIC 3.0 security capabilities applicable to the use case are not dependent on a data transfer mechanism. In other words, the same security capabilities apply if the conveyance is over leased lines, software virtual private network (VPN), hardware VPN, etc.

The following are assumptions about the agency campus.

- The agency campus accesses the web or trusted external partners through a TIC access point.
- The agency maintains control over and has significant visibility into the agency campus.
- Data is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- The agency employs network operation center (NOC) and security operation center (SOC) tools capable of maintaining and protecting the portions of the overall infrastructure. To accomplish this, agencies can opt to use a NOC and SOC, or commensurate solutions.

The following are assumptions about the TIC access point.

- The TIC access point is TIC 2.2 compliant.
- The TIC access point is managed as a Single Service TICAP by the agency, or as a Multi-Service TICAP by the agency, another agency, or an MTIPS provider.
- The agency employs traditional methods for accessing the TIC access point, though supplemental protections may be provided using alternative methods.

The following are assumptions about external partners (e.g., a CSP, a network, an extranet).

- The agency ensures that interactions with external partners follow agency-defined policies and procedures for business need justification, partner connection eligibility, service levels, data protections, incident response information sharing and reporting, costs, data ownership, and contracting.
- The agency uses only limited and well-defined services of external partners or permits external partners access to only limited and well-defined services of the agency.

[3] "National Cybersecurity Protection System," Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[4] "Continuous Diagnostics and Mitigation," Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cdm.

- The agency has limited control over and visibility into external partners.
- External partners have NOCs and SOCs that control and protect the portions of their infrastructure where the agency has little to no control or visibility.
- The agency only uses secure mechanisms (e.g., transport layer security (TLS) or VPN) to communicate with external partners.
- The agency only uses strong authentication mechanisms (e.g., Federal Information Processing Standard (FIPS) 140-2[5] complaint multi-factor authentication (MFA)) with external partners.
- Data provided to external partners is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.

The following are assumptions about partner agencies.

- The partner agency employs appropriate TIC use cases for all its external network connections, ensuring appropriate protections and information sharing with NCPS.
- Interactions with partner agencies follow agency-defined policies and procedures for business need justification, partner connection eligibility, service levels, data protections, incident response information sharing and reporting, costs, data ownership, and contracting.
- The agency uses only limited and well-defined services of partner agencies or permits partner agencies access to only limited and well-defined services of the agency.
- The agency has limited control over and visibility into partner agencies.
- Partner agencies have NOCs and SOCs that control and protect the portions of their infrastructure where the agency has little to no control or visibility.
- The agency only uses using secure mechanisms (e.g., TLS or VPN) to communicate with partner agencies.
- The agency only uses strong authentication mechanisms (e.g., FIPS 140-2 complaint MFA) with partner agencies.
- Data provided to partner agencies is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.

The following are assumptions about the web.

- The web contains untrusted entities.
- The agency cannot apply policy in the web.

The following are assumptions about the public user.

- The public user is accessing agency services from the internet.
- The public user is unmanaged and untrusted by the agency.

5. Conceptual Architecture

The Traditional TIC Use Case focuses on the scenario in which agency network traffic traverses a TIC access point when moving to and from external zones. As shown in Figure 3, this use case is composed primarily of six trust zones: agency campus, TIC access point, web, public user, external partner, and partner agency TIC access point. These trust zones are detailed in Table 2. To simplify the visualization and descriptions, the use case shows single trust zones to represent classes of external entities or environments. However, this simplification is not meant to imply that an agency must treat all entities and environments of the same class (e.g., external partners) in the same manner.

[5] Federal Information Processing Standard 140-2," National Institute of Standards and Technology (2019). https://csrc.nist.gov/publications/detail/fips/140/2/final.

The traditional TIC model was commonly represented as comprising an "Internal Zone," containing agency components and the TIC access point as its boundary, and an "External Zone," containing the various entities the agency would communicate with[6]. This model is conceptualized in TIC 3.0 by nesting trust zones within a larger, primary trust zone, which is depicted as the Agency Trust Zone in Figure 3. In this scenario, the nested trust zones include the agency campus, the TIC access point, the branch office, and the remote user. These trust zones can be nested within the Agency Trust Zone because they share a boundary that is secured by the same PEP (i.e., the TIC access point).

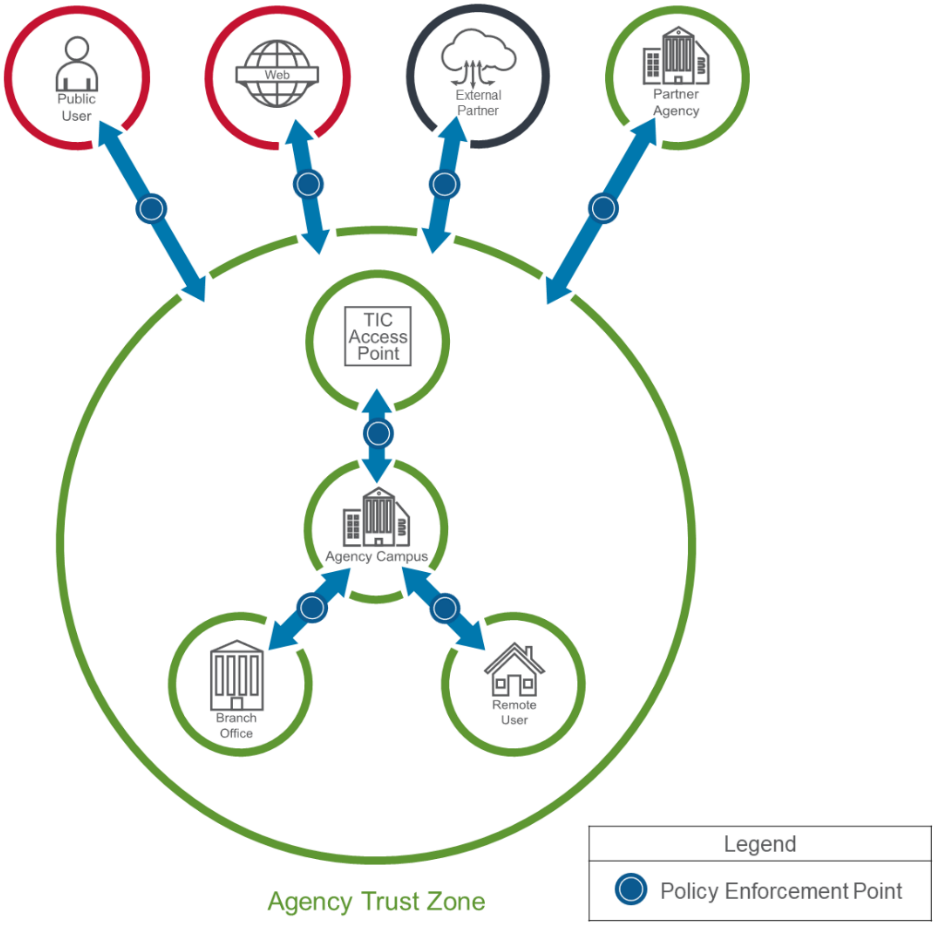


Figure 3: Traditional TIC Conceptual Architecture

The branch office and remote user trust zones are included in this use case because they are commonly deployed when implementing TIC 2.2. In the TIC 2.2 model, those zones send traffic to external entities through agency TIC access points.

It is important to note that the architecture depicted in Figure 3 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 consider the TIC access point as being outside the Agency Trust Zone,

[6] "TIC Reference Architecture v2.2," Department of Homeland Security (2017). https://www.cisa.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf.

or as a PEP rather than a distinct zone. Also, some agencies' deployments of the Traditional TIC Use Case may include only a subset of the listed trust zones.

The trust zones are labeled with levels of trust, using the three-level example trust hierarchy from the Reference Architecture. While these levels were selected based on existing pilots or deployments, they may not capture the needs or requirements of all agencies. As such, agencies may determine and label trust zones according to the trust levels that best describe their environment. For example, an agency may not consider the partner agency as having a high trust level and may decide to label it with a medium trust level.

The trust levels in this use case are intended to be examples. Agencies may define and assign trust levels to align with their requirements, environments, and risk tolerance.

Table 2 briefly explains why each entity is labeled with either a high, medium, or low trust zone in this use case to help agencies determine what is most appropriate in their implementation.

Table 2: Trust Zones in the Traditional TIC Use Case

Trust Zone	Description
Agency Campus Trust Zone	The Agency Campus Trust Zone is the logical zone for the agency campus or the agency's enterprise network. The trust zone includes management entities (MGMTs) such as the NOC, SOC, and other entities. The agency maintains control over and visibility into the agency campus. It is responsible for defining policies, implementing them in the various PEPs controlled by the agency, and identifying and responding to incidents. Given the control and visibility maintained by the agency, the Agency Campus Trust Zone is labeled with a ***high trust level*** in this use case.
TIC Access Point Trust Zone	The TIC Access Point Trust Zone is the logical zone that depicts the location where the agency campus's external connections are consolidated. The TIC access point must have, at a minimum, TIC 2.2 security controls in place to secure and monitor the traffic entering and leaving the agency campus. This trust zone may be part of the agency campus as its TICAP or may be provided by an external entity as part of an MTIPS solution or a Multi-Service TICAP. The TIC Access Point Trust Zone may also host agency services for use by external entities. While the agency may have limits in terms of control and visibility into this zone, the TIC Access Point Trust Zone is labeled with a ***high trust level*** in this use case due to the well-defined security protections and NCPS telemetry employed by the TIC access point.
Agency Trust Zone	The Agency Trust Zone is a logical zone that represents the accreditation boundary for the agency. It contains smaller, nested trust zones, including the agency campus and the TIC access point; it may also include branch offices and remote users. This zone may not exist in some agencies' implementation or may contain different components. For example, some agencies may not consider the TIC access point, branch offices, or remote users inside a common boundary. Given that it is comprised of zones labeled with high trust levels, the Agency Trust Zone is labeled with a ***high trust level*** in this use case.

Trust Zone	Description
Web Trust Zone	The Web Trust Zone is a logical zone that depicts an environment containing untrusted external services that agency users may access, with no PEPs or MGMTs where the agency, or entities acting on its behalf, may deploy policies. Given these limitations, the Web Trust Zone is labeled with a ***low trust level*** in this use case.
Public User Trust Zone	The Public User Trust Zone is a logical zone that depicts an untrusted and unmanaged user of agency services with no PEPs or MGMTs where the agency, or entities acting on its behalf, may deploy policies. Given these limitations, the Public User Trust Zone is labeled with a ***low trust level*** in this use case.
External Partner Trust Zone	The External Partner Trust Zone is a logical trust zone for an external partner that offers services to or receives services from the agency. The agency has limited control over and visibility into the external partner environment. The agency can provide certain defined capabilities for an external partner to manage, and the external partner is responsible for protecting the underlying infrastructure. The trust zone may include a MGMT with functions locally scoped for the environment. The PEP between the external partner and the agency campus may use a shared responsibility deployment model, with hardware owned and managed by the TICAP and services deployed by the agency. Given the more limited control and visibility available to the agency, the External Partner Trust Zone is labeled with a ***medium trust level*** in this use case.
Partner Agency Trust Zone	The Partner Agency Trust Zone is a logical trust zone for a government agency that partners with the agency in support of mission objectives and business operations. The agency has limited control and visibility into the partner agency, assuming the partner agency employs one or more TIC use cases for its connectivity and ensures appropriate protections and telemetry for NCPS. Both the agency and the partner agency maintain PEPs covering traffic between these trust zones. While the agency has similar limits in terms of control and visibility as the external partner, the Partner Agency Trust Zone is labeled with a ***high trust level*** in this use case due to its similar security protections and NCPS telemetry.
Branch Office Trust Zone	The Branch Office Trust Zone is a logical trust zone showing a common TIC 2.2 use case where a branch office routes its traffic through the agency's TIC access point. Given the control and visibility maintained by the agency, the Branch Office Trust Zone is labeled with a ***high trust level*** in this use case.
Remote User Trust Zone	The Remote User Trust Zone is a logical trust zone showing a common TIC 2.2 use case where a remote user connects to the agency campus via a VPN, or similar, and routes its traffic through the agency's TIC access point with a logical separation maintained between the remote user's system and the agency campus network. Given the control and visibility maintained by the agency, the Remote User Trust Zone is labeled with a ***high trust level*** in this use case.

6. Security Patterns

Four security patterns capture the data flows for the Traditional TIC Use Case. Each has distinct sources, destinations, and options for policy enforcement. Regardless of the options chosen, due diligence must be practiced, ensuring agencies are protecting their information in line with their risk tolerances. When additional security capabilities are necessary to manage residual risk, agencies should apply the controls or explore options for compensating capabilities that achieve the same protections to manage risks.

The security patterns include the following trust zone destinations:

- Web,
- Public user,
- External partner, and
- Partner agency

6.1 Security Pattern 1: Agency Campus to Web

Figure 4 illustrates connections where agency entities connect to the open internet or web for services. Connections in this security pattern are among the riskiest because the web is an untrusted entity; therefore, the greatest amount of rigor should be applied to the security capabilities. In this security pattern, the PEP at the agency campus applies any applicable security policies and ensures the appropriate traffic is forwarded to the TIC access point. Then, the TIC access point applies all applicable security policies before transiting traffic to or from the web.

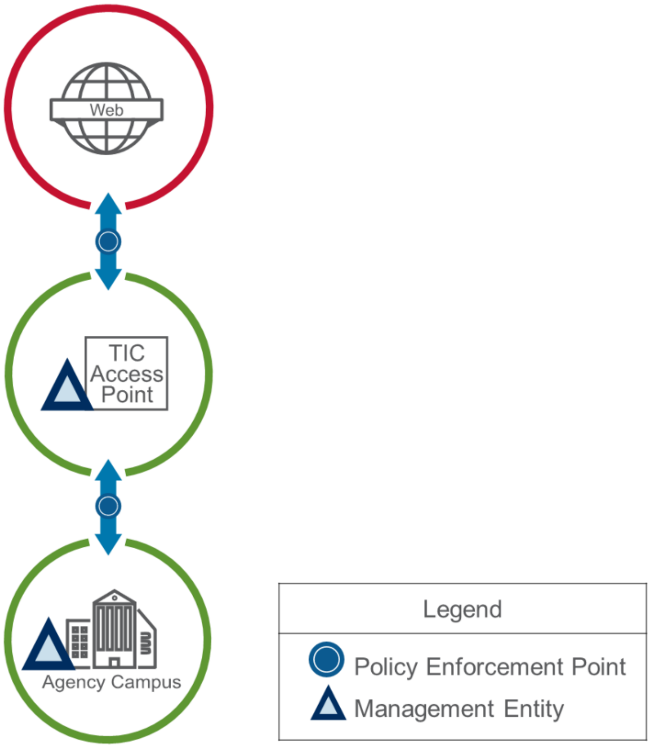


Figure 4: Security Pattern 1: Agency Campus to Web

Implementation Consideration

Agencies should apply the greatest rigor to security capabilities for the connections between the agency campus and the web.

6.2 Security Pattern 2: Public User to Agency Campus

Figure 5 illustrates connections where a public user accesses services provided by the agency, commonly in the form of web services. Connections in this security pattern are among the riskiest since a possibly untrusted public user is connecting to the agency and its services; therefore, the greatest amount of rigor should be applied to the security capabilities. Since users are accessing services that may contain agency data, agencies must practice due diligence in protecting their information in line with their risk tolerances.

In this security pattern, the PEP at the agency campus applies any applicable security policies and ensures the relevant service traffic is forwarded to the TIC access point. This PEP also ensures that data flows to and from public users are properly protected and only authorized services and information are exchanged with eligible users. The TIC access point applies all applicable security policies before transiting traffic to and from the public user.

If an agency service is deployed to the TIC access point, the PEP may be a shared responsibility deployment model, with hardware owned and managed by the TICAP and services deployed by the agency. In this scenario, the TIC access point ensures that only appropriate traffic is sent to the agency services, and the agency ensures that only authorized users can access and exchange authorized information with the agency services.

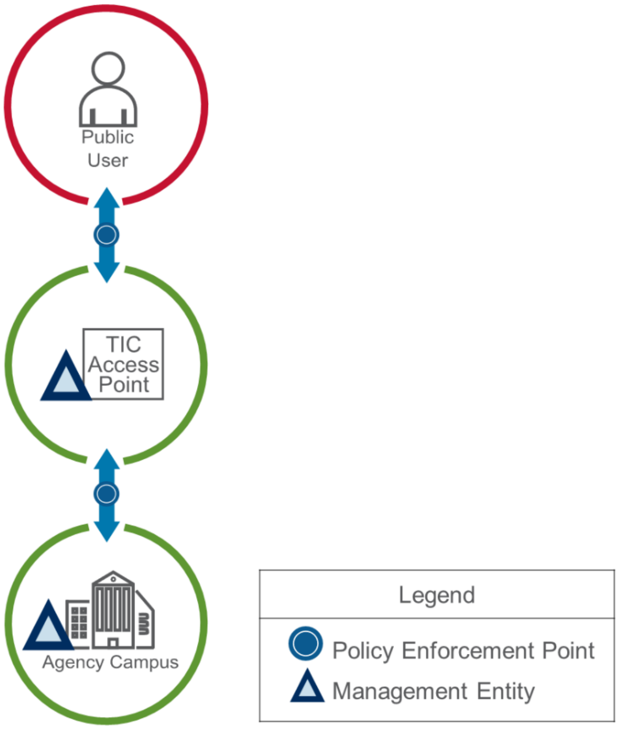


Figure 5: Security Pattern 2: Public User to Agency

Implementation Consideration

Agencies should apply the greatest rigor to security capabilities where public users access agency services. Information must be protected in line with their risk tolerances.

6.3 Security Pattern 3: Agency Campus to External Partner

Figure 6 illustrates the scenario where an agency uses the services of or provides services to an external partner. Entities within the agency campus either establish a new protected connection or use an existing protected connection with the external partner to access resources from that partner.

In this security pattern, the PEP at the agency campus ensures that data flows to and from external partners are properly protected and only authorized services and information are being exchanged. The PEP at the agency campus applies any applicable security policies and ensures the appropriate traffic is forwarded to the TIC access point. The TIC access point applies all applicable security policies before transiting traffic to or from the external partner.

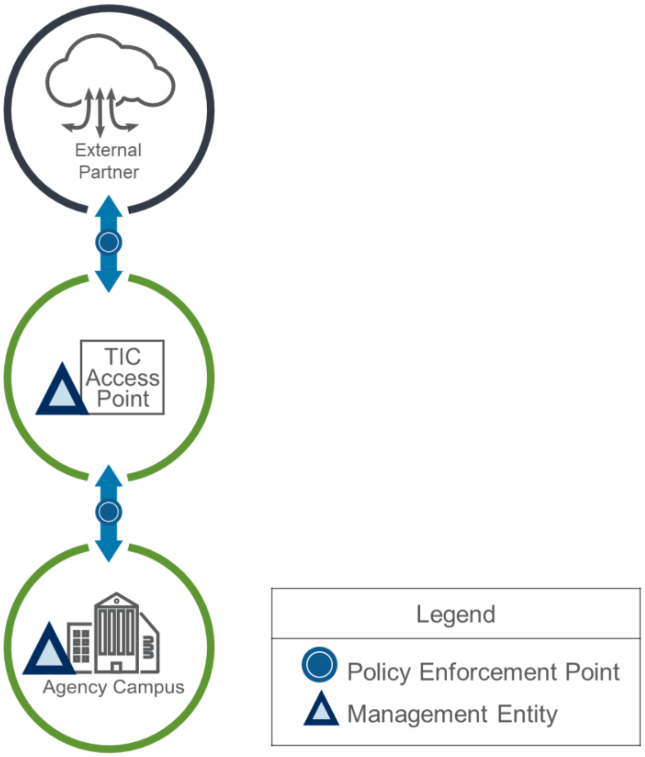


Figure 6: Security Pattern 3: Agency to External Partner

Implementation Consideration

Agencies must ensure that (1) appropriate protections are in place when connecting with an external partner and (2) only authorized services are being used and authorized information is being exchanged.

6.4 Security Pattern 4: Agency Campus to Partner Agency

Figure 7 illustrates connections where an agency connects to or provides services to a partner agency (e.g., interagency traffic). This communication can take place through two options, described below. Regardless of the option chosen, due diligence must be practiced to ensure agencies are protecting their information in line with their risk tolerances. One option permits a direct network connection to the partner agency. The partner agency employs appropriate TIC use cases for all its external network connections, ensuring a baseline of protections along with information sharing with NCPS. However, agencies may supplement these protections to better reflect their risk tolerances.

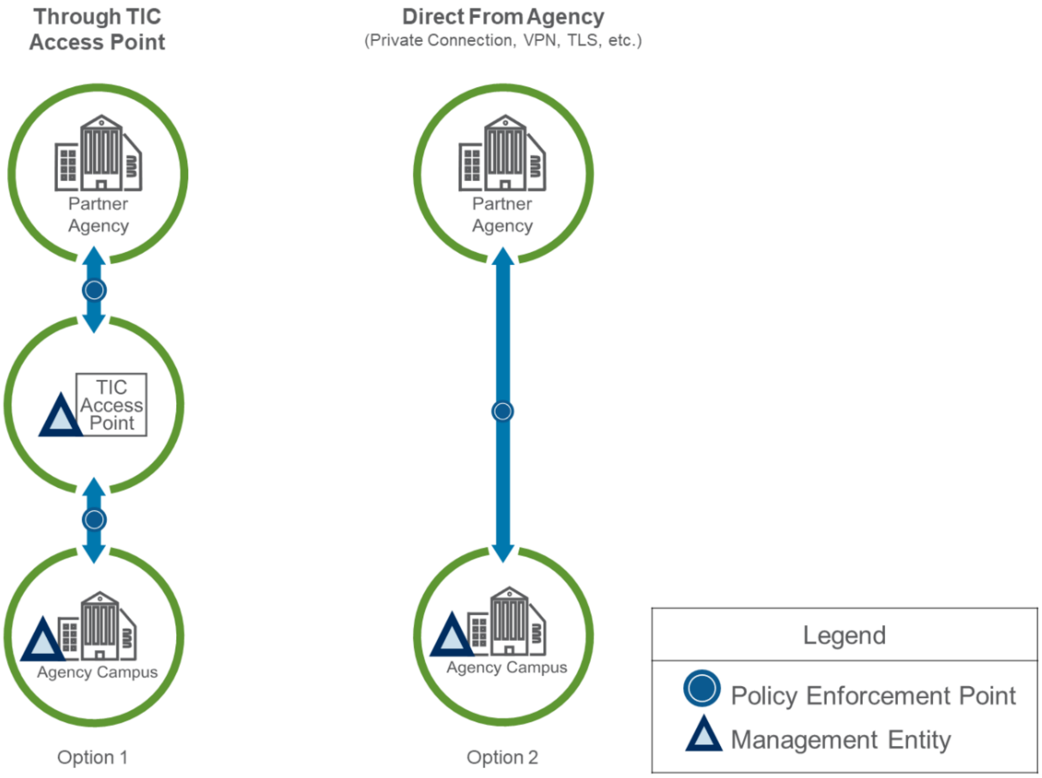
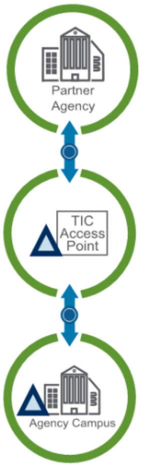


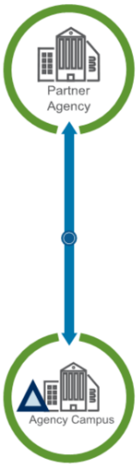
Figure 7: Security Pattern 4: Agency Campus to Partner Agency

Implementation Consideration

Agencies may connect directly with partner agencies so long as NCPS visibility exists at both ends.



The **first option** (left) has traffic flowing between the agency campus and the partner agency through a TIC access point. Entities within the agency campus either establish a protected connection to the partner agency or make use of an existing protected connection established with the partner agency. Agency and partner agency resources can then be accessed through this protected channel. The PEP at the agency campus and the TIC access point ensure that data flows to and from partner agencies are properly protected and only authorized services and information are being exchanged.



The **second option** (left) consists of a direct connection from the agency campus to the partner agency. Entities within the agency campus either establish a protected connection to the partner agency or use an existing protected connection established with the partner agency. Agency and partner agency resources can then be accessed through this protected channel. These protected channels may go through a private connection between the agency and the partner agency, or through shared infrastructure like the internet.

The PEP at the agency campus ensures proper traffic forwarding, such that only authorized traffic is forwarded to the partner agency. This PEP also ensures that connections for flows are properly protected and only authorized services and information is exchanged with the partner agency.

This option permits a direct network connection to the partner agency. The partner agency employs appropriate TIC use cases for all its external network connections, ensuring appropriate protections and information sharing with NCPS. However, agencies may supplement these protections to better reflect their risk tolerances. The agency or partner agency may provide telemetry from this option to NCPS.

7. Applicable Security Capabilities

The Traditional TIC Use Case draws on security capabilities from both the new and legacy TIC guidance. The list of security capabilities in the legacy *TIC Reference Architecture v2.2* outlines the requirements to secure, manage, and operate a TIC access point. The Security Capabilities Catalog contains a broader set of security capabilities that agencies can use to accomplish TIC objectives across TIC use cases. While the TIC 2.2 security capabilities can provide protection for most, agencies may supplement the existing TIC 2.2 security capabilities with new TIC 3.0 security capabilities to reflect their agency requirements, risk tolerances, and other factors.

Unlike the TIC 2.2 security capabilities, TIC 3.0 security capabilities are not prescriptive, but rather are descriptive, allowing for flexibility in implementation. Appendix B provides mappings between the TIC 2.2 and TIC 3.0 security capabilities, for reference.

The sections below explain how existing TIC 2.2 security capabilities at a TIC access point can be used as part of agency implementations of TIC 3.0 security capabilities.

7.1 Universal Security Capabilities

The Security Capabilities Catalog contains a table of universal security capabilities that apply across TIC use cases. Agencies can determine the level of rigor that is applied to these security capabilities such that it is in line with their agency risk tolerances and federal guidelines. Unique application guidance for the universal security capabilities in the Traditional TIC Use Case is outlined in Table 3.

Agencies may determine the level of rigor that is applied to these security capabilities based on their agency risk tolerance and federal guidelines.

Table 3: Universal Security Capabilities

Universal Security Capabilities

Capability	Description	Use Case Specific Guidance
Backup and Recovery	Backup and recovery entails keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.	TIC access points handle backup and recovery of configuration and data for their systems and services. If agencies deploy services to the TIC access point or provide configuration or data to a TIC access point, agencies should include those services, configurations, or data in their backup and recovery routines.
Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	TIC access points centralize and analyze their internally collected logs. If possible, agencies should integrate telemetry available from TIC access points to their central log management and analysis environment.
Configuration Management	Configuration management is the implementation of a formal plan for documenting and managing changes to the environment, and monitoring for deviations, preferably automated.	TIC access points implement a formal plan for configuration management for their systems and services. If agencies deploy services to the TIC access point or provide configuration or data to a TIC access point, agencies should handle changes to these services, configuration, or data through their formal configuration management plan.

Capability	Description	Use Case Specific Guidance
Incident Response Planning and Incident Handling	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.	TIC access points implement incident response plans covering incidents discovered or occurring in the TIC access point. Agencies should work with the TICAP to ensure that the SOC and NOC working on their behalf coordinates any incident response activities with the TIC access point.
Inventory	Inventory entails developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and restricted from gaining access.	TIC access points maintain inventories of their systems, services, and entities. Agencies should maintain an inventory of their connections to TIC access points as well as any external partners, partner agencies, and any agency services deployed to the TIC access point.
Least Privilege	Least privilege is a design principle whereby each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	TIC access points are configured according to least privilege. Agencies should apply least privilege to any services deployed to the TIC access point and users permitted access to TIC access point systems and services.
Secure Administration	Secure administration entails performing administrative tasks in a secure manner, using secure protocols.	TIC access points are configured to use secure administration. Agencies should use secure administration practices when administering any systems or services they have administrative privilege for in TIC access points.
Strong Authentication	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	TIC access points are configured to use strong authentication for internal systems. Agencies should use strong authentication when accessing any systems or services in TIC access points, including any agency services deployed to the TIC access point.

Capability	Description	Use Case Specific Guidance
Time Synchronization	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clock times and enable accurate comparison of timestamps between systems.	TIC access points maintain time synchronization across their systems. If possible, agencies should synchronize their systems, including agency services deployed to the TIC access point, to integrate the telemetry from TIC access points.
Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	TIC access points conduct regular active and passive security reviews to discover and mitigate risks in the TIC access point. Each agency's NOC and SOC should include TIC access points in the security reviews of their agency.
Patch Management	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	TIC access points handle patch management for systems and services that support it (e.g., firewalls, SIEMs, etc.). Agencies may need to handle patch management for agency services deployed to the TIC access point.
Auditing and Accounting	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	TIC access points maintain audit and record access. To facilitate agency auditing and accounting, agencies should integrate the records from TIC access points into their own record-keeping system.
Resilience	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	TIC access points have resilience features including uninterrupted power, diverse routes, and in the case of some TIC access points, geographic diversity. Agencies should understand the resilience provided by their TIC access point, and, if possible, have multiple routes to their TIC access point.

Capability	Description	Use Case Specific Guidance
Enterprise Threat Intelligence	Enterprise threat intelligence is the usage of threat intelligence from private or government sources to implement mitigations for the identified risks.	TIC access points can integrate threat intelligence from outside sources. Agencies should understand the threat intelligence sources TIC access points employ and may supplement the intelligence if needed.
Situational Awareness	Situational awareness is maintaining effective current and historical awareness across all components.	TIC access points maintain situational awareness across customers. If possible, agencies should integrate telemetry available from TIC access points—including telemetry from agency services deployed in the TIC access point—into the platforms they use to maintain situational awareness, to improve their overall situational awareness.
Dynamic Threat Discovery	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	TIC access points provide telemetry to an agency for use in their dynamic threat discovery program.
Policy Enforcement Parity	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding path, or endpoints used.	This capability is commonly implemented by having agency entities route traffic through agency TIC access points when communicating with the web or external partners. When working with a partner agency, this capability is implemented by ensuring both agencies use appropriate TIC protections for their external connections.
Effective Use of Shared Services	Effective use of shared services means that shared services are employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	This capability has been commonly implemented using shared infrastructure when implementing Single Service TICAPs or using Multi-Service TICAPs.

Capability	Description	Use Case Specific Guidance
Integrated Desktop, Mobile, and Remote Policies	Integrated desktop, mobile, and remote policies define and enforce policies that apply to a given agency entity independent of its location.	This capability has been commonly implemented by having all agency entities route traffic through agency TIC access points when communicating with the web or external partners.

7.2 Policy Enforcement Point Security Capabilities

PEP security capabilities focus on the network-level and inform technical implementation for a given use case, such as securing agency campus communication with agency-sanctioned external partners. Agencies have the discretion to determine the applicability and level of rigor necessary for applying PEP security capabilities based on their mission, the policy enforcement options available, federal guidelines, and risk tolerance. From the Security Capabilities Catalog, the PEP security capability groups applicable to this use case correspond to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- Domain Name System (DNS),
- Intrusion Detection,
- Enterprise,
- Unified Communications and Collaboration (UCC), and
- Data Protection.

> Agencies may determine the applicability and rigor of the security capabilities based on federal guidelines, mission needs, available policy enforcement options, and risk tolerance.

The PEP security capability listing is not exhaustive. Additional security capabilities may be deployed by agencies to reflect their risk tolerances, early adoption of security capabilities, the maturity level of existing cyber programs, and other factors.

Table 4: Files PEP Security Capabilities

Files PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	TIC access points can apply anti-malware protections in their email services (see Table 5) and web traffic (see Table 6).
Content Disarm and Reconstruction	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Detonation Chamber	Detonation chambers facilitate the detection of malicious code using protected and isolated execution environments to analyze the files.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Data Loss Prevention	Data loss prevention (DLP) technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TIC access points employ DLP programs. Agencies should understand the protections offered by the TIC access point's DLP program and integrate them into their overall DLP program.

Table 5: Email PEP Security Capabilities

Email PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	Agencies can use email services in TIC access points, which provide anti-phishing protections.
Anti-spam Protections	Anti-spam protections detect and quarantine instances of spam.	Agencies can use email services in TIC access points, which provide spam detection and quarantine services.
Authenticated Received Chain	Authenticated received chain allows for an intermediary, like a mailing list or forwarding service, to sign its own authentication of the original email, allowing downstream entities to accept the intermediary's authentication even if the email was changed.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TIC access points employ DLP programs. Agencies should understand the protections offered by the TIC access point's DLP program and integrate them into their overall DLP program.

Capability	Description	Use Case Specific Guidance
Domain Signature Verification for Incoming Email	Domain signature verification protections authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol defined in Request for Comments (RFC) 7489.[7]	Agencies can use email services in TIC access points, which can perform integrity checks, using schemes like DomainKeys Identified Mail (DKIM) or Sender Policy Framework (SPF), on incoming email.
Domain Signatures for Outgoing Email	Domain signature protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures according to the DMARC email authentication protocol that is defined in RFC 7489.	Agencies can use email services in TIC access points, which can digitally sign outbound email using schemes like DKIM.
Encryption for Email Transmission	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Malicious Link Protections	Malicious link protections detect malicious links in emails and prevent users from accessing them.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Link Click-through Protection	Link click-through protections ensure that when a link from an email is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
EINSTEIN 3 Accelerated Email Protections	EINSTEIN 3 Accelerated (E^3A)[8] is an intrusion prevention capability offered by NCPS, provided by CISA, that includes an email filtering security service.	Agencies can use email services in TIC access points, which support the integration of NCPS E^3A email protections.

[7] "Domain-based Message Authentication, Reporting, and Conformance Request for Comments: 7489," Internet Engineering Task Force (2015). https://tools.ietf.org/html/rfc7489.

[8] "EINSTEIN 3 Accelerated," Cybersecurity and Infrastructure Security Agency (2013). https://www.cisa.gov/publication/einstein-3-accelerated.

Table 6: Web PEP Security Capabilities

Web PEP Security Capabilities[9]

Capability	Description	Use Case Specific Guidance
Break and Inspect	Break and Inspect systems, or encryption proxies, terminate encrypted traffic, log or perform policy enforcement against the plaintext, and re-encrypt the traffic, if applicable, before transmitting to the final destination.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities. Break and Inspect solutions should be considered in the context of the sensitivity of data being scanned, the trust level designation of the source and destination, other security capabilities that offer comparable visibility, and the protocols and services in use.
Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	TIC access points can detect and remove malicious content in web traffic.
Certificate Denylisting	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	TIC access points can detect and remove malicious content in web traffic.
Authenticated Proxy	Authenticated proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TIC access points employ DLP programs, and agencies should understand the protections offered by the TIC access point's DLP program and integrate them into their overall DLP program.

[9] TIC 2.2 includes a variety of protections for unencrypted web traffic, which may be supplemented depending on the use of encrypted web traffic used by an agency.

Capability	Description	Use Case Specific Guidance
Domain Resolution Filtering	Domain resolution filtering prevents entities from using the DNS-over-Hypertext Transfer Protocol Secure (HTTPS), or DoH, domain resolution protocol, possibly evading DNS-based protections.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, like those documented by the Internet Engineering Task Force (IETF).[10]	TIC access points employ proxies for web traffic which ensures compliance of the web sessions.
Domain Category Filtering	Domain category filtering technologies allow for classes of domains (e.g., banking, medical) to receive a different set of security protections.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Domain Reputation Filtering	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Bandwidth Control	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	TIC access points can detect and remove malicious content in web traffic.
Access Control	Access control technologies allow an agency to define policies that limit what actions may be performed by connected users and entities.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

[10] "RFCs," Internet Engineering Task Force (2021). https://www.ietf.org/standards/rfcs/

Table 7: Network PEP Security Capabilities

Network PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Access Control	Access control protections prevent the ingress, egress, or transmission of unauthorized network traffic.	TIC access points employ a combination of firewalls and proxies to limit the traffic coming into and leaving the TIC access point. When VPNs, or similar technologies, are used to bridge together the agency campus network with other environments, the agency campus should use access control protections to ensure only appropriate traffic is sent to and received from the other environments.
Internet Address Denylisting	Internet address denylisting protections prevent the ingest or transiting of traffic received from, or destined, to a denylisted internet address.	TIC access points can drop web traffic to specific IP addresses and can alert on attempts to access specific IP addresses.
Host Containment	Host containment protections enable a network to revoke or quarantine a host's access to the network.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Network Segmentation	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	TIC access points employ network segmentation internally. By routing their external connections through TIC access points, agencies can segment their networks from external environments. When VPNs, or similar technologies, are used to bridge together the agency campus network with other environments, the agency campus network should be segmented so that least privilege access is maintained, and to limit the impact of the compromise of the external environment.

Capability	Description	Use Case Specific Guidance
Micro-segmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Table 8: Resiliency PEP Security Capabilities

Resiliency PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Distributed Denial of Service Protections	Distributed Denial of Service (DDoS) protections mitigate the effects of distributed denial of service attacks.	TIC access points provide DDoS protections.
Elastic Expansion	Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Regional Delivery	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Table 9: Domain Name System PEP Security Capabilities

Domain Name System PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Domain Name Sinkholing	Domain name sinkholing protections are a form of denylisting that protects clients from accessing malicious domains by responding to DNS queries for those domains.	Agencies can use DNS resolution services in TIC access points, which provide DNS sinkholing.

Capability	Description	Use Case Specific Guidance
Domain Name Verification for Agency Clients	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to Domain Name System Security Extensions (DNSSEC).	Agencies can use DNS resolution services in TIC access points, which provide DNSSEC verification.
Domain Name Validation for Agency Domains	Domain name validation protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution to the domain names.	Agencies can use DNS hosting services in the TIC access point, which support DNSSEC.
EINSTEIN 3 Accelerated Domain Name Protections	E^3A is an intrusion prevention capability offered by NCPS, provided by CISA, that includes a DNS sinkholing security service.	Agencies can use DNS resolution services in TIC access points, which can support the integration of NCPS E^3A DNS protections.

Table 10: Intrusion Detection PEP Security Capabilities

Intrusion Detection PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Endpoint Detection and Response	Endpoint detection and response (EDR) tools combine endpoint and network event data to aid in the detection of malicious activity.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Intrusion Detection and Prevention Systems	Intrusion detection systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity.	TIC access points pass network traffic through intrusion detection systems. When VPNs, or similar technologies, are used to bridge together the agency campus network with other environments, the agency campus should ensure that traffic to and from the external environment are passed through an intrusion detection and prevention system.

Capability	Description	Use Case Specific Guidance
Adaptive Access Control	Adaptive access control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Deception Platforms	Deception platform technologies provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Certificate Transparency Log Monitoring	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Table 11: Enterprise PEP Security Capabilities

Enterprise PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Security Orchestration, Automation, and Response	Security Orchestration, Automation, and Response (SOAR) tools define, prioritize, and automate the response to security incidents.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Shadow Information Technology Detection	Shadow information technology (IT) detection systems detect the presence of unauthorized software and systems in use by an agency.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Capability	Description	Use Case Specific Guidance
Virtual Private Network	VPN solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	TIC access points provide VPN services with varying levels of protection applied, depending on the entity that the VPN tunnel is established with. When VPNs, or similar technologies, are used to bridge the agency campus network with other environments, the agency campus network should apply network segmentation, application gateways, virtual desktop infrastructure (VDI), etc. to ensure least privilege access is maintained and to limit the impact of a compromise of the other environment.

Table 12: Unified Communications and Collaboration PEP Security Capabilities

Unified Communications and Collaboration PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Identity Verification	Identity verification ensures that access to the virtual meeting is limited to appropriate individuals. Waiting room features, where the meeting host authorizes vetted individuals to join the meeting, can also be utilized.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Encrypted Communication	Communication between virtual meeting participants and any data exchanged is encrypted at rest and in transit. Some UCC offerings support end-to-end encryption, where encryption is performed on the clients and can only be decrypted by the other authenticated participants and cannot be decrypted by the UCC vendor.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Connection Termination	Connection termination mechanisms ensure the meeting host can positively control participation through inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Capability	Description	Use Case Specific Guidance
Data Loss Prevention	Mechanisms should be implemented to control the sharing of information between UCC participants, intentional or incidental. This may be integrated into additional agency DLP technologies and can include keyword matching, attachment file type or existence prohibitions, attachment size limitations, or even audio/visual filters.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

Table 13: Data Protection PEP Security Capabilities

Data Protection PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Access Control	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Protections for Data in Transit	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TIC access points employ DLP programs, and the agency should understand the protections offered by the TIC access point's DLP program and integrate them into the agency's overall DLP program.
Data Access and Use Telemetry	Data access and use telemetry identifies agency-sensitive data stored, processed, or transmitted, including those located at a service provider, and enforces detailed logging for access or changes to sensitive data.	New capability in TIC 3.0 that can be implemented to supplement the TIC 2.2 capabilities.

8. Telemetry Requirements

Figure 8 shows the conceptual architecture of the Traditional TIC Use Case with the telemetry requirements. These flows indicate when an agency should share telemetry with CISA. In the Traditional TIC Use Case, there are two types of telemetry that might get shared: CDM telemetry and NCPS telemetry. Most traditional TIC deployments have CDM telemetry shared with CISA by capabilities deployed on the agency campus, and NCPS telemetry is shared with CISA from the TIC access points. Agencies may provide telemetry for direct connections to partner agencies by working with NCPS. Consult the NCPS program[11] and CDM program[12] for further details.

Agencies share telemetry information with CISA through multiple programs, as coordinated directly, to ensure visibility and situational awareness are preserved and shared protections can be maintained.

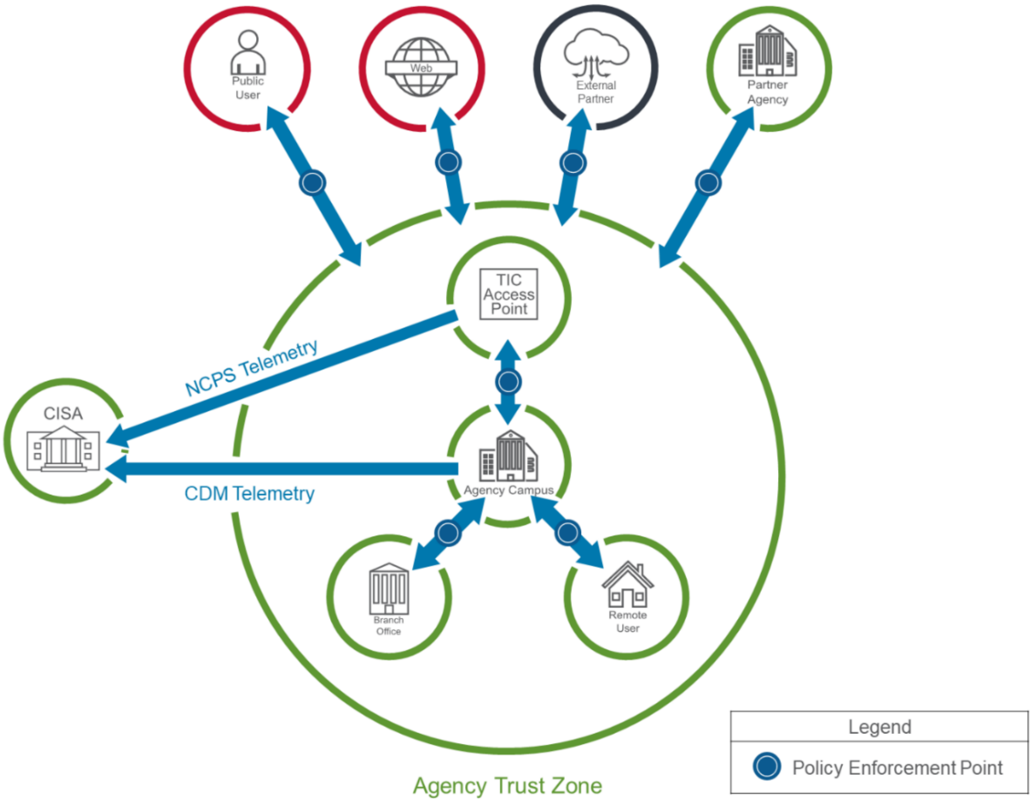


Figure 8: Traditional TIC Telemetry Sharing with CISA

[11] "National Cybersecurity Protection System (NCPS)", Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/national-cybersecurity-protection-system-ncps.

[12] "Continuous Diagnostics and Mitigation (CDM)", Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/cdm.

9. Conclusion

Traditional TIC Use Case defines how network security should be applied when an agency has personnel in a physical location (i.e., an agency campus) that uses a TIC access point, either an agency TIC Access Provider (TICAP) or Managed Trusted Internet Protocol Services (MTIPS), when accessing the web, trusted external partners, or partner government agencies. This document provides guidance on how an agency can configure its traditional TIC data flows and apply relevant TIC 3.0 security capabilities. It considers four security patterns relevant to the traditional TIC deployment:

- Secure agency campus access to web;
- Public user to secure agency campus;
- Secure agency campus access to agency-sanctioned external partners; and
- Secure agency campus access to partner agencies.

This use case should be considered the default use case, as defined by OMB M-19-26 and used in conjunction with the Security Capabilities Catalog and other TIC 3.0 guidance documentation.

Appendix A – Glossary and Definitions

This glossary contains terms and definitions that are used across the TIC documents and not necessarily applicable to all use cases.

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, and 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.

Appendix B – Mapping TIC 2.2 Capabilities and TIC 3.0 Capabilities

The security capabilities included in the legacy *TIC Reference Architecture v2.2* outlined requirements for security, managing, and operating a TIC access point. The security capabilities included in the *TIC 3.0 Security Capabilities Catalog* provide a list of security capabilities that are applicable across TIC 3.0 use cases.

Appendix B.1 – TIC 2.2 Capabilities to TIC 3.0 Capabilities

The following table show how the TIC 2.2 security capabilities map to the TIC 3.0 security capabilities. The mapping is not intended to be a strict mapping or to define equivalence of capabilities, but rather these tables can provide a reference for current MTIPS providers, TICAPs, and agencies.

Table 14: TIC 2.2 Capabilities to TIC 3.0 Capabilities

TIC 2.2 Capabilities to TIC 3.0 Capabilities

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TS.PF.01	**Secure all TIC Traffic**	Enterprise Threat Intelligence, Policy Enforcement Parity	Networking: Access Control and Network Segmentation
TS.PF.02	**Default Deny**	Not applicable	Networking: Access Control and Network Segmentation
TS.PF.03	**Stateless Filtering**	Not applicable	Networking: Access Control and Network Segmentation, Internet Protocol Denylisting
TS.PF.04	**Stateful Filtering**	Not applicable	Networking: Access Control and Network Segmentation
TS.PF.05	**Filter by Source Address**	Not applicable	Networking: Access Control and Network Segmentation
TS.PF.06	**Asymmetric Routing**	Not applicable	Networking: Access Control and Network Segmentation
TS.PF.07	**H.323**	Not applicable	Not applicable

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TS.CF.01	**Application Layer Filtering**	Not applicable	Web: Request for Comments Compliance Enforcement
TS.CF.02	**Web Session Filtering**	Not applicable	Files: Anti-malware Email: Uniform Resource Locator Click-through Protection Web: Active Content Mitigation, Content Filtering, Domain Category Filtering, Domain Reputation Filtering, Malicious Content Filtering
TS.CF.03	**Web Firewall**	Not applicable	Not applicable
TS.CF.04	**Mail Filtering**	Not applicable	Files: Anti-malware Email: Anti-phishing Protections, Anti-spam Protections, Malicious Uniform Resource Locator Protections
TS.CF.05	**Agency Specific Mail Filters**	Not applicable	Files: Anti-malware
TS.CF.06	**Incoming Mail Authentication (Mail Forgery Detection)**	Not applicable	Email: Domain Signature Verification for Incoming Email
TS.CF.07	**Email Authentication (Digitally Signing Mail)**	Not applicable	Email: Domain Signatures for Outgoing Email
TS.CF.08	**Mail Quarantine**	Not applicable	Not applicable

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TS.CF.09	**Routing Protocol Authentication (BGP Protection)**	Secure Administration	Networking: Access Control, Network Segmentation
TS.CF.10	**Reducing Cleartext**	Secure Administration	Not applicable
TS.CF.11	**Encrypted Traffic Inspection**	Policy Enforcement Parity	Not applicable
TS.CF.12	**Custom Malware and Content Filtering**	Not applicable	Files: Anti-malware
TS.CF.13	**DNS Filtering**	Not applicable	Domain Name System: Domain Name Sinkholing, Domain Name Verification for Agency Clients
TS.CF.14	**Loose/Strict Source Filtering**	Not applicable	Not applicable
TS.INS.01	**NCPS**	Not applicable	Mail: EINSTEIN 3 Accelerated Email Protections Domain Name System: EINSTEIN 3 Accelerated Domain Name Protections Intrusion Detection: Intrusion Detection and Prevention Systems
TS.INS.02	**IDS/NIDS**	Enterprise Threat Intelligence	Not applicable
TS.RA.01	**Agency-User Remote Access (Filter by Source Address)**	Strong Authentication	Enterprise: Virtual Private Network
TS.RA.02	**External Dedicated Access**	Strong Authentication	Enterprise: Virtual Private Network

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TS.RA.03	**Extranet Dedicated Access**	Strong Authentication	Enterprise: Virtual Private Network
TM.AU.01	**User Authentication**	Strong Authentication	Not applicable
TM.PC.01	**TIC Facility**	Resilience	Not applicable
TM.PC.02	**NOC/SOC Facilities**	Not applicable	Not applicable
TM.PC.03	**SCIF Facilities**	Not applicable	Not applicable
TM.PC.04	**Dedicated TIC Spaces**	Not applicable	Not applicable
TM.PC.05	**Facility Resiliency**	Not applicable	Not applicable
TM.PC.06	**Geographic Diversity**	Resilience	Not applicable
TM.TC.01	**Route Diversity**	Resilience	Not applicable
TM.TC.02	**Least Functionality**	Least Privilege	Not applicable
TM.TC.03	**IPv6**	Policy Enforcement Parity	Not applicable
TM.TC.04	**DNS Authoritative Servers (DNSSEC)**	Not applicable	Domain Name System: Domain Name Validation for Agency Domains
TM.TC.05	**Response Authority**	Incident Response Planning and Incident Handling, Enterprise Threat Intelligence	Not applicable
TM.TC.06	**TIC Staffing**	Incident Response Planning and Incident Handling	Not applicable
TM.TC.07	**Response Access**	Incident Response Planning and Incident Handling	Not applicable
TM.COM.01	**TIC and NCCIC (TS/SCI)**	Incident Response Planning and Incident Handling	Not applicable

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TM.COM.02	**TIC and Customer**	Incident Response Planning and Incident Handling	Not applicable
TM.COM.03	**TIC and NCCIC (SECRET)**	Incident Response Planning and Incident Handling	Not applicable
TM.DS.01	**Storage Capacity**	Central Log Management with Analysis, Situational Awareness	Not applicable
TM.DS.02	**Back-up Data**	Backup and Recovery, Incident Response Planning and Incident Handling	Not applicable
TM.DS.03	**Data Ownership**	Not applicable	Not applicable
TM.DS.04	**Data Attribution & Retrieval**	Effective Use of Shared Services	Not applicable
TM.DS.05	**DLP**	Not applicable	Files: Data Loss Prevention Email: Data Loss Prevention Web: Data Loss Prevention
TM.LOG.01	**NTP Server**	Time Synchronization, Central Log Management with Analysis	Not applicable
TM.LOG.02	**Time Stamping**	Time Synchronization, Central Log Management with Analysis	Not applicable
TM.LOG.03	**Session Traceability**	Auditing and Accounting, Situational Awareness, Central Log Management with Analysis	Not applicable

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TM.LOG.04	**Log Retention**	Auditing and Accounting, Situational Awareness, Central Log Management with Analysis	Not applicable
TO.RES.01	**Response Timeframe**	Incident Response Planning and Incident Handling, Enterprise Threat Intelligence	Not applicable
TO.RES.02	**Response Guidance**	Incident Response Planning and Incident Handling, Enterprise Threat Intelligence	Not applicable
TO.RES.03	**Denial of Service Response**	Not applicable	Resiliency: Distributed Denial of Service Protections
TO.MG.01	**System Inventory**	Inventory	Not applicable
TO.MG.02	**Configuration & Change Management**	Configuration Management	Not applicable
TO.MG.03	**Change Communication**	Configuration Management	Not applicable
TO.MG.04	**Contingency Planning**	Incident Response Planning and Incident Handling	Not applicable
TO.MG.05	**TSP**	Not applicable	Not applicable
TO.MG.06	**Maintenance Scheduling**	Configuration Management	Not applicable
TO.MG.07	**Custom Agency Networks**	Inventory	Not applicable
TO.MG.08	**SLA**	Not applicable	Not applicable
TO.MG.09	**Exception Process**	Not applicable	Not applicable

Capability ID	Short Title	Universal Capabilities (potentially partial)	PEP Capabilities (potentially partial)
TO.MG.10	**Tailored Security Policies**	Not applicable	Not applicable
TO.MG.11	**Tailored Communications**	Not applicable	Not applicable
TO.MON.01	**Situational Awareness**	Central Log Management with Analysis, Situational Awareness	Not applicable
TO.MON.02	**Vulnerability Scanning**	Vulnerability Management	Not applicable
TO.MON.03	**Audit Access**	Auditing and Accounting	Not applicable
TO.MON.04	**Log Sharing**	Auditing and Accounting, Central Log Management with Analysis	Not applicable
TO.MON.05	**Operational Exercises**	Vulnerability Management	Not applicable
TO.REP.01	**Customer Service Metrics**	Auditing and Accounting	Not applicable
TO.REP.02	**Operational Metrics**	Auditing and Accounting	Not applicable
TO.REP.03	**Customer Notification**	Auditing and Accounting, Incident Response Planning and Incident Handling	Not applicable
TO.REP.04	**Incident Reporting**	Auditing and Accounting, Incident Response Planning and Incident Handling	Not applicable

Appendix B.2 – TIC 3.0 Capabilities to TIC 2.2 Capabilities

The following tables show the reverse mapping; how the TIC 3.0 security capabilities map to the TIC 2.2 security capabilities. The mappings are broken down by universal capabilities and PEP capabilities. The mapping is not intended to be a strict mapping or to define equivalence of capabilities, but rather these tables can provide a reference for current MTIPS providers, TICAPs, and agencies.

Table 15: Universal TIC 3.0 Capabilities to TIC 2.2 Capabilities

Universal TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Backup and Recovery	Backup and recovery entails keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.	TM.DS.02
Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and the security analysis aids in discovery and response to malicious activity.	TO.MON.01 TO.MON.04 TM.DS.01 TM.LOG.*11F[13]
Configuration Management	Configuration management is the implementation of a formal plan for documenting and managing changes to the environment, and monitoring for deviations, preferably automated.	TO.MG.02 TO.MG.03 TO.MG.06
Incident Response Planning and Incident Handling	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.	TM.TC.05 TM.TC.06 TM.TC.07 TM.COM.01 TM.COM.02 TM.COM.03 TO.RES.01 TO.RES.02 TO.MG.04 TM.DS.02 TO.REP.03 TO.REP.04

[13] All TM.LOG capabilities in Section B of the *TIC Reference Architecture v 2.2*.

Capability	Description	TIC 2.2 Mapping
Inventory	Inventory entails developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and restricted from gaining access.	TO.MG.01 TO.MG.07
Least Privilege	Least privilege is a design principle applied to security architectures such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	TM.TC.02
Secure Administration	Secure administration entails performing administrative tasks in a secure manner, using secure protocols.	TS.CF.10 TS.CF.09
Strong Authentication	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	TM.AU.01 TS.RA.*12F[14]
Time Synchronization	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clock times and enable accurate comparison of timestamps between systems.	TM.LOG.01 TM.LOG.02
Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	TO.MON.02 TO.MON.05
Patch Management	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	See Configuration Management and Vulnerability Management.
Auditing and Accounting	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	TO.MON.03 TO.MON.04 TM.LOG.03 TM.LOG.04 TO.MG.07 TO.REP.01 TO.REP.02 TO.REP.03 TO.REP.04

[14] All TS.RA capabilities in Section B of the *TIC Reference Architecture v 2,2*.

Capability	Description	TIC 2.2 Mapping
Resilience	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	TM.TC.01 TM.PC.01 TM.PC.06
Enterprise Threat Intelligence	Enterprise threat intelligence is a way to obtain threat intelligence from private and government sources and to implement mitigations for the identified risks.	TO.RES.02 TS.PF.01 TS.INS.02 TO.RES.01 TM.TC.05 TM.COM.*13F[15]
Situational Awareness	Situational awareness is maintaining effective awareness, both current and historical, across all components.	TO.MON.01 TM.DS.01 TM.LOG.03 TM.LOG.04
Dynamic Threat Discovery	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	Not applicable
Policy Enforcement Parity	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding path, or endpoints used.	TS.PF.01 TS.CF.11 TM.TC.03
Effective Use of Shared Services	Effective use of shared services means that shared services should be employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	TM.DS.04
Integrated Desktop, Mobile, and Remote Policies	Integrated desktop, mobile, and remote policies define and enforce policies that apply to a given agency entity independent of its location.	Not applicable

[15] All TM.COM capabilities in Section B of the TIC 2.2 Reference Architecture.

Table 16: Files PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Files PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	TS.CF.02 TS.CF.04 TS.CF.05 TS.CF.12
Content Disarm and Reconstruction	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	Not applicable
Detonation Chamber	Detonation chambers facilitate the detection of malicious code using protected and isolated execution environments to analyze the files.	Not applicable
Data Loss Prevention	Data loss prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TM.DS.05

Table 17: Email PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Email PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	TS.CF.04
Anti-spam Protections	Anti-spam protections detect and quarantine instances of spam.	TS.CF.04
Authenticated Received Chain	Authenticated received chain allows for an intermediary, like a mailing list or forwarding service, to sign its own authentication of the original email, allowing downstream entities to accept the intermediary's authentication even if the email was changed.	Not applicable
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TM.DS.05

Capability	Description	TIC 2.2 Mapping
Domain Signature Verification for Incoming Email	Domain signature verification protections authenticate incoming email according to the DMARC email authentication protocol defined in RFC 7489.	TS.CF.06
Domain Signatures for Outgoing Email	Domain signature protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures according to the DMARC email authentication protocol is defined in RFC 7489.	TS.CF.07
Encryption for Email Transmission	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	Not applicable
Malicious Link Protections	Malicious link protections detect malicious links in emails and prevent users from accessing them.	Not applicable
Link Click-through Protection	Link click-through protections ensure that when a link from an email is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	Not applicable
EINSTEIN 3 Accelerated Email Protections	E^3A is an intrusion prevention capability, offered by NCPS, provided by CISA, that includes an email filtering security service.	TS.INS.01

Table 18: Web PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Web PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Break and Inspect	Break and Inspect systems, or encryption proxies, terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.	Not applicable
Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	TS.CF.02 TS.CF.04

Capability	Description	TIC 2.2 Mapping
Certificate Denylisting	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	Not applicable
Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	TS.CF.02 TS.CF.04
Authenticated Proxy	Authenticated proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	Not applicable
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TM.DS.05
Domain Resolution Filtering	Domain resolution filtering prevents entities from using the DNS-over- Hypertext Transfer Protocol Secure (HTTPS), or DoH, domain resolution protocol, possibly evading DNS-based protections.	Not applicable
Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, documented by the IETF.	TS.CF.01
Domain Category Filtering	Domain category filtering technologies allow for classes of domains (e.g., banking, medical) to receive a different set of security protections.	Not applicable
Domain Reputation Filtering	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	Not applicable
Bandwidth Control	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	Not applicable
Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	TS.CF.02 TS.CF.04
Access Control	Access control technologies allow an agency to define policies limiting what actions may be performed by connected users and entities.	Not applicable

Table 19: Networking PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Networking PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Access Control	Access control protections prevent the ingress, egress, or transiting of unauthorized network traffic.	TS.PF.01-06 TS.CF.09
Internet Address Denylisting	Internet address denylisting protections prevent the ingest or transiting of traffic received from or destined to a denylisted internet address.	TS.PF.03 TS.CF.02 TS.CF.04 TS.INS.01
Host Containment	Host containment protections enable a network to revoke or quarantine a host's access to the network.	Not applicable
Network Segmentation	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	TS.PF.01-06 TS.CF.09
Micro-segmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	Not applicable

Table 20: Resiliency PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Resiliency PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Distributed Denial of Service Protections	DDoS protections mitigate the effects of distributed denial of service attacks.	TO.RES.03
Elastic Expansion	Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.	Not applicable
Regional Delivery	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	Not applicable

Table 21: DNS PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

DNS PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Domain Name System Sinkholing	Domain name sinkholing protections are a form of denylisting that protects clients from accessing malicious domains by responding to DNS queries for those domains.	TS.CF.13
Domain Name Verification for Agency Clients	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to DNSSEC.	TS.CF.13
Domain Name Validation for Agency Domains	Domain name validation protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution to the domain names.	TM.TC.04
EINSTEIN 3 Accelerated Domain Name Protections	E^3A is an intrusion prevention capability offered by NCPS, provided by CISA that includes a DNS sinkholing security service.	TS.INS.01

Table 22: Intrusion Detection PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Intrusion Detection PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Endpoint Detection and Response	Endpoint detection and response tools combine endpoint and network event data to aid in the detection of malicious activity.	Not applicable
Intrusion Detection and Prevention Systems	Intrusion detection and prevention systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity.	TS.INS.01
Adaptive Access Control	Adaptive access control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	Not applicable

Capability	Description	TIC 2.2 Mapping
Deception Platforms	Deception platform technologies provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.	Not applicable
Certificate Transparency Log Monitoring	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	Not applicable

Table 23: Enterprise PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Enterprise PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Security Orchestration, Automation, and Response	SOAR tools define, prioritize, and automate the response to security incidents.	Not applicable
Shadow Information Technology Detection	Shadow IT detection systems detect the presence of unauthorized software and systems in use by an agency.	Not applicable
Virtual Private Network	VPN solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	TS.RA.01 TS.RA.02 TS.RA.03

Table 24: Unified Communications and Collaboration PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Unified Communications and Collaboration PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Identity Verification	Identity verification ensures that access to the virtual meeting is limited to appropriate individuals. Waiting room features, where the meeting host authorizes vetted individuals to join the meeting, can also be utilized.	Not applicable

Capability	Description	TIC 2.2 Mapping
Encrypted Communication	Communication between virtual meeting participants and any data exchanged is encrypted at rest and in transit. Some UCC offerings support end-to-end encryption, where encryption is performed on the clients and can only be decrypted by the other authenticated participants and cannot be decrypted by the UCC vendor.	Not applicable
Connection Termination	Mechanisms that ensure the meeting host can positively control participation. These can include inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	Not applicable
Data Loss Prevention	Mechanisms should be implemented to control information sharing between UCC participants, intentional or incidental. This may be integrated into other DLP solutions, including keyword matching, attachment file type or existence prohibitions, attachment size limitations, or audio/visual filters.	Not applicable

Table 25: Data Protection PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Data Protection PEP TIC 3.0 Capabilities to TIC 2.2 Capabilities

Capability	Description	TIC 2.2 Mapping
Access Control	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	Not applicable
Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	Not applicable
Protections for Data in Transit	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	Not applicable
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	TM.DS.05
Data Access and Use Telemetry	Data access and use telemetry identifies agency-sensitive data stored, processed, or transmitted, including those located at a service provider, and enforcing detailed logging for access or changes to sensitive data.	Not applicable