Trusted Internet Connections 3.0

TIC Core Guidance Volume 2:

Reference Architecture

July 2021

Version 1.1

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Revision History

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

Table 1: Revision History

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

Reader's Guide

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

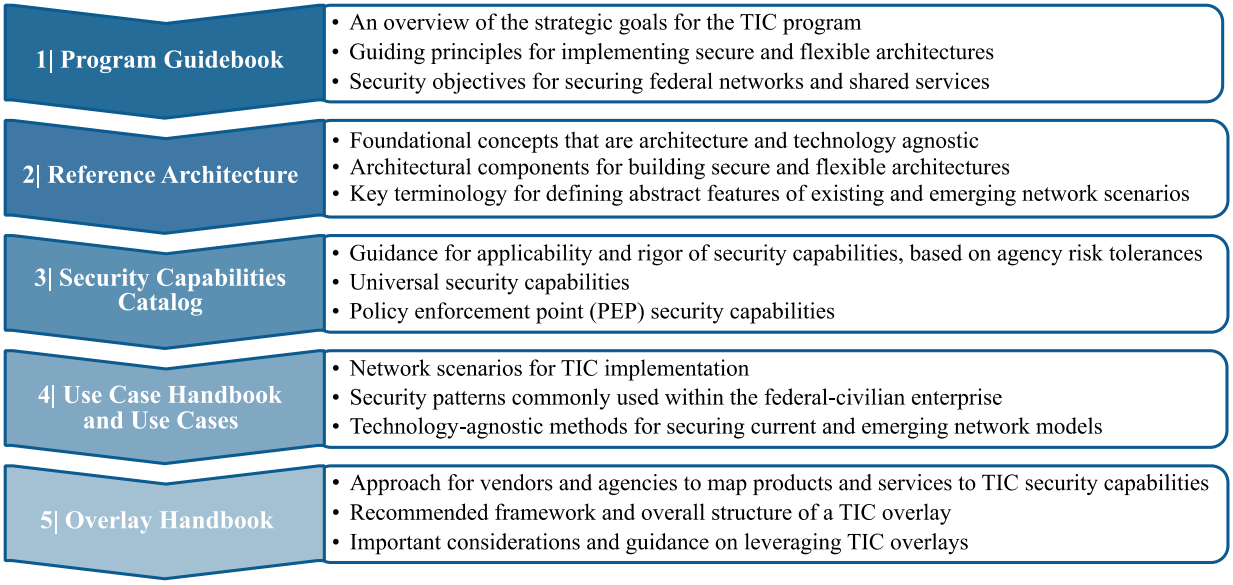

Figure 1: TIC 3.0 Guidance Snapshot

TIC 3.0 Reference Architecture

Table of Contents

List of Figures

List of Tables

1. Introduction

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

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

1.1 Key Terms

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

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

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

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

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

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

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

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

---

[1] "Update to the Trusted Internet Connections (TIC) Initiative," Office of Management and Budget M-19-26 (2019). https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf.

[2] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

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

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

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

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

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

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

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

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

2. Purpose of the Reference Architecture

The purpose of the *TIC 3.0 Reference Architecture* (Reference Architecture) is to provide high-level guidance for the application of the TIC program and establish foundational components that build security patterns found in TIC use cases. The Reference Architecture can be leveraged to:

- Serve as a foundation for solutions,
- Be used for comparison and alignment purposes,
- Provide common language and terminology,
- Ensure consistency of technological implementations,
- Support solution validation,
- Justify budget and acquisition requests, and
- Encourage adherence to common standards, specifications, and patterns.

3. Security Objectives of TIC 3.0

As the Federal Government continues to expand into cloud and mobile environments, an agency's assets, data, and components are commonly located in areas beyond their network boundary – on remote devices, at cloud data centers, with external partners, etc. To protect these dispersed assets, the TIC program defines encompassing security objectives to guide agencies in securing their network traffic. The objectives intend to limit the likelihood of a cybersecurity event. Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected.

Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected.

The TIC security objectives should be viewed independently of the types of traffic being secured, but different types of traffic influence how the objectives are interpreted. Each objective stands on its own, independent of the other objectives. They should not be considered an order-of-operations. In other words, the intent of the objectives is not to suggest that an agency must execute one objective to execute another.

The TIC objectives, described in Table 2, are intended to set expectations for architectures, guide implementation, and establish clear goals at the network level. The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones or stored at either or both trust zones.

Table 2: TIC 3.0 Security Objectives

Objective[3]	Description
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures

4. Key Concepts of TIC 3.0

The following key concepts are used to develop TIC 3.0 conceptual architectures and use cases. The concepts are intentionally abstract to provide context for capability implementation as well as coverage across a wide variety of platforms, services, and environments. TIC security pattern diagrams encapsulate each of the following key concepts:

- Security capabilities,
- Policy enforcement points,
- Trust zones, and
- Management entities.

[3] The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones or stored at either or both trust zones.

4.1 Security Capabilities

The security capabilities listed in the *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog) define the protections foundational to the TIC initiative. The National Institute of Standards and Technology (NIST) defines a security capability as a combination of mutually reinforcing security controls implemented by technical, physical, and procedural means.[4] Security capabilities help to define and provide protections for information being processed, stored, or transmitted by information systems.

There are a variety of security protections performed as data or traffic moves between endpoints; Figure 2 uses circles to represent the security protections along the connecting arrow between endpoints. Each capability increases the trust in a given data flow. To focus security on an endpoint and closer to the data, it may be better to place capabilities closer to the server or client side of the connection.

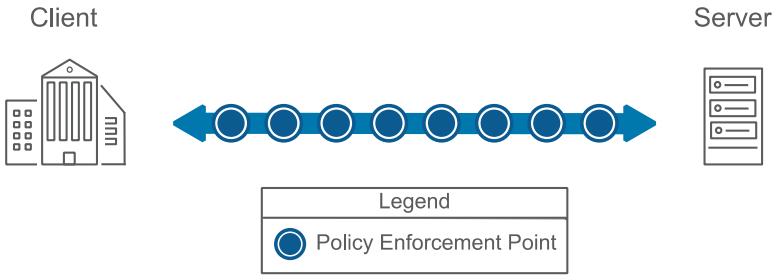

Figure 2: Security Capabilities Are Positioned Along Data Flows

4.2 Policy Enforcement Points

In TIC 3.0, security capabilities are applied by policy enforcement points (PEPs), which may be security devices, tools, services, or applications that enforce the security capabilities. Enforcement may occur at any point between endpoints. Enforcement actions include permit, deny, modify, redirect, delay, and other forms of data manipulation. The actions are initiated based on a variety of attributes, as defined in security policies.

Each PEP applied to a data flow provides different assurances, based on different attributes (e.g., state, confidence, transparency, control, etc.). With PEPs chained in series, strategically placed, and executing properly, an endpoint can have confidence, once all the capabilities have been applied, that the data conforms to a known set of parameters. This change in confidence is represented in Figure 3 by the change in colors along the data flow where the confidence increases after data moves from client to server through the PEPs.

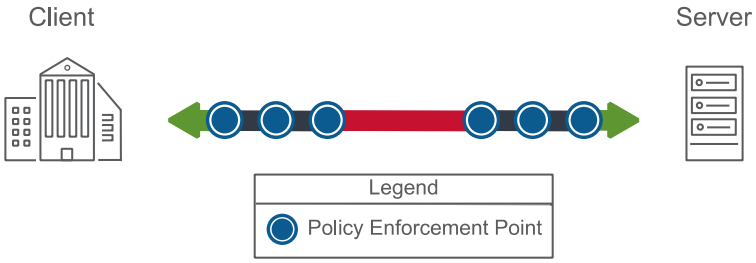

Figure 3: PEP Protections Affect Trust

[4] "Standards for Security Categorization of Information and Information Systems," Federal Information Processing Standards (FIPS) PUB 199 (2004): Page 4. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

Multiple capabilities can be applied at a common PEP, or location, in the path of the data flow. This may be to improve performance, to provide an auditable demarcation point, or for other reasons. Alternatively, some PEPs may only meet a subset of the applicable security capabilities and can be combined with complimentary PEPs to meet all capabilities. This is shown below in Figure 4 by grouping the capability circles.

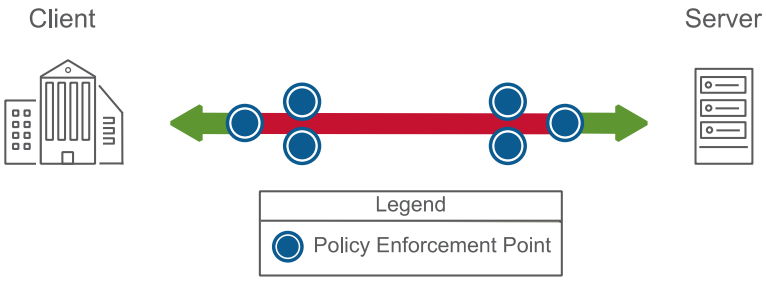

Figure 4: PEP Capabilities Grouped into Shared Positions

4.3 Trust Zones

A single element or group of elements with shared security capability protections constitute a trust zone. This zone is a discrete computing environment involved in information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the zone. The Reference Architecture uses circles to depict unique trust zones as shown in Figure 5.

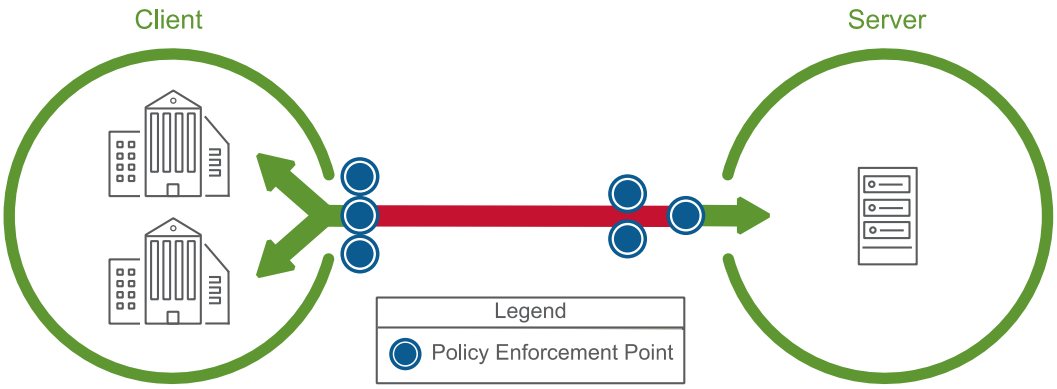

Figure 5: Endpoints Sharing PEP Positions Make Up A Trust Zone

Within a trust zone, further segmentation is permissible, including segmentation to the network, application, or browser level. This can occur when there are both shared protections that are common across all entities within the trust zone and distinct capabilities that are applicable only to a subset of endpoints within that zone (as shown below in Figure 6). Agencies may use relevant factors for grouping endpoints, which could include client purpose, services, user roles, need-to-know, geography, or other criteria.

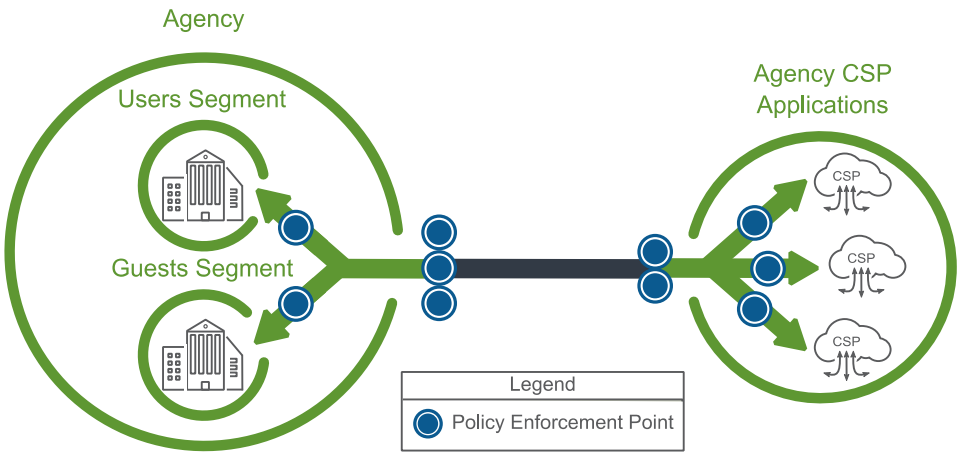

Figure 6: Segmentation Within a Trust Zone

Alternatively, these segments may be considered as trust zones themselves. They can still share common PEP capabilities with other trust zones while also retaining the ability to apply zone-unique protections, as shown in Figure 7. By extension, individual endpoints and workloads may be considered as trust zones themselves, in line with zero trust principles.

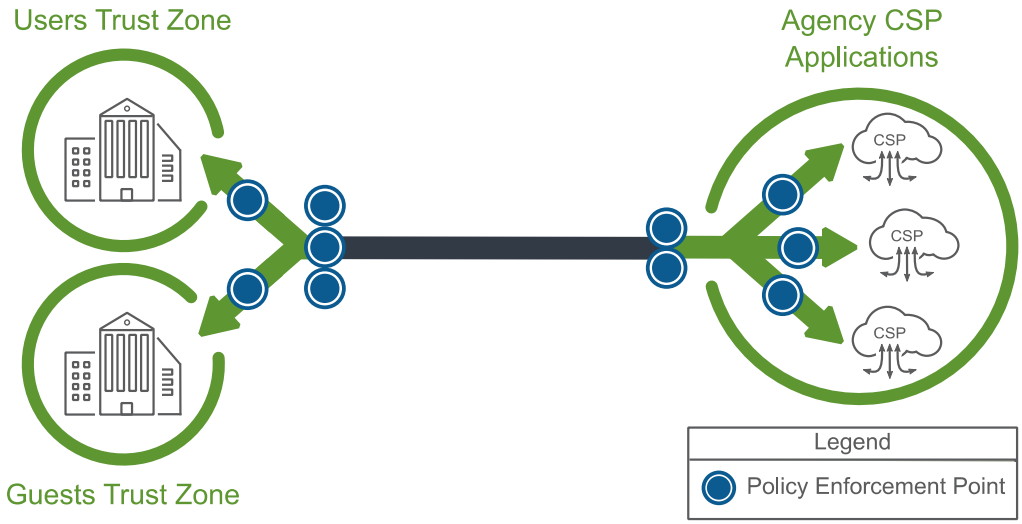

Figure 7: Segments as Separate Trust Zones

4.3.1 Trust Levels

Trust zones are designated with a trust level as a way of describing and facilitating understanding about the relative rigor or robustness that should be employed when implementing applicable security capabilities. The Reference Architecture makes use of three designations — high, medium, and low — to depict groupings within the trust gradient from full trust to lack of trust, respectively. **These three levels, depicted in Figure 8, should only be considered an *example* of how an agency can define different trust levels.**

Figure 8: Example Trust Zone Gradient

Agencies can use a categorization or gradient scheme most appropriate for their environment. For example, an agency could have eight categories of trust versus the three used here. Sample considerations for designating levels of trust are detailed in Section 4.3.2.

Agencies are encouraged to determine the trust levels or categories most appropriate for their environment.

This trust level concept can be aligned with traditional concepts of network boundary trust, but it also permits a more fine-grained approach (e.g. aligning with the concepts of zero trust), depending on how an agency might best understand and describe their environment. A trust zone does not necessarily inherit trust and security from an adjacent trust zone, nor does the trust and the subsequent security capabilities depend on the trust of the adjacent zone.

Levels of trust may also be factors in deployment options for services or data. By deploying security capabilities and ensuring a rigor of implementation commensurate with the level of trust designated to a zone, an agency may use the increased assurance as an opportunity to deploy services or more sensitive data to the zone. This deployment may increase the impact of compromise for the zone, but the increased security capabilities applied to the zone can help manage the risk.

4.3.2 Trust Level Considerations

Table 3 shows some *sample* considerations to provide agencies with a framework when thinking about trust levels within their environments, enabling them to more effectively implement TIC security capabilities. Table 3 provides considerations for defining the trust level of a zone using the three levels used as examples throughout the Reference Architecture (e.g., high, medium, or low). The considerations are based on an agency's level of control, transparency, and verification.

Table 3: Sample Trust Considerations

TRUST CONSIDERATIONS	High Trust	Medium Trust	Low Trust
Control: What degree of control does an agency have over the environment's security policies, procedures, and practices?	An agency has ***significant control*** over the environment (e.g., a physical appliance hosted on agency premises).	An agency has ***some degree of control*** over the environment (e.g., an agency instance within cloud and mobile environment).	An agency has ***little to no control*** over the environment (e.g., an application as a service).
Transparency: What degree of visibility does an agency have into the environment?	An agency has ***significant visibility*** into the environment (e.g., an environment is housed within an agency's on-premise network).	An agency has ***partial visibility*** into the environment (e.g., an environment is housed within an agency instance or cloud and mobile environment).	An agency has ***limited visibility*** into the environment (e.g., an environment is fully maintained and managed by another entity).
Verification: To what extent can an agency verify an environment's compliance with relevant controls, standards, and/or best practices?	An agency can ***continuously validate*** the environment's compliance (e.g., through continuously-collected data or application programming interfaces (APIs).	An agency can ***periodically validate*** *the* environment's compliance (e.g., through annual audit).	An agency ***does not have access to information*** validating the environment's compliance.

The considerations presented above are not prescriptive, but rather facilitate decision-making in determining the appropriate level of trust within a given environment and the consequent level of rigor to employ when implementing security capabilities. The trust level designation for a zone should reflect its risk posture; agencies are responsible for implementing protections that are commensurate with the designated trust level of a zone and its security risks. Agencies should consider any unique variables (e.g.,

as required by the Federal Information Security Modernization Act of 2014[5], Risk Management Framework,[6] etc.) when making their trust level determinations.

Agencies are responsible for implementing protections that are commensurate with the designated trust level of a zone and its security risks.

Figure 9 below provides examples of high, medium, and low trust zones. This figure is meant to highlight that the same type of environment can have a different trust level designation depending on an agency's considerations for a specific scenario. For example, an agency could determine that all cloud service providers (CSPs) should be designated as medium trust. On the other hand, an agency could also categorize one CSP as medium trust and another as low trust based on unique circumstances, like stronger contractual terms that provide greater visibility into one of the CSPs.

Figure 9: Trust Level Designation Examples

4.3.3 Management Entities

Management entities (MGMT) control the collection, processing, analysis, and display of information collected from the PEPs and allows information technology professionals to control devices on the network. MGMTs provide agencies and CISA with the visibility to identify cybersecurity risks. The MGMT represents entities such as:

- organizations (e.g., network operations centers/security operations centers, policy compliance offices, etc.) and
- products and/or services (e.g., cloud services, cloud access security broker (CASB), security information and event management (SIEM), security dashboards, etc.).

The oversight and analytics capabilities of the MGMT, such as response functionality, are essential components of TIC. The MGMT maintains communications with one or more of the PEPs within a given agency architecture, receiving artifacts such as alerts, system inventories, and capability status. These artifacts provide visibility into the agency's environment and security posture. The TIC guidance does not detail the telemetry that agencies need to provide to CISA programs such as NCPS and CDM. Since

[5] Federal Information Security Modernization Act (P.L. 113-283), December 2014.

[6] "Risk Management," National Institute of Standards and Technology (2019). https://csrc.nist.gov/Projects/Risk-Management/rmf-overview.

visibility needs will often align, this telemetry may be used for both CISA and agency purposes. Agencies remain free to address any unique telemetry requirements beyond those from CISA.

5. Conceptual Implementation of TIC 3.0

To conceptually implement the key concepts defined in the previous section, the TIC 3.0 guidance leverages security patterns and use cases. These tools support the flexibility embedded into the guidance by allowing agencies options for implementing TIC 3.0.

5.1 Security Patterns

A security pattern describes an end-to-end data flow between 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 trust zones. These patterns abstract the path of the data flow, along with the underlying PEPs and trust zones that the data might traverse. Figure 10 shows an example security pattern between an agency branch office and the web.

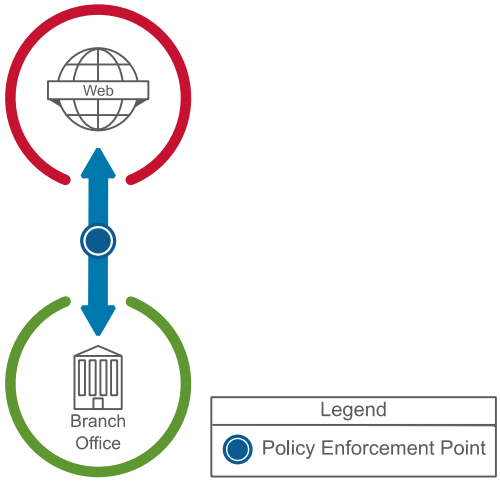

Figure 10: Example Security Pattern

The abstract nature of the security patterns allows for a diversity of implementation options. These options may augment the capabilities or guidance for the security pattern with their own specific capabilities or implementation guidance.

Figure 11 provides an example set of implementation options for the security pattern in Figure 10. While common implementation options may be included, their inclusion is not meant to preclude agencies from implementing other options based on their specific needs. Agencies are encouraged to explore the variety of security patterns typically included in TIC use cases.

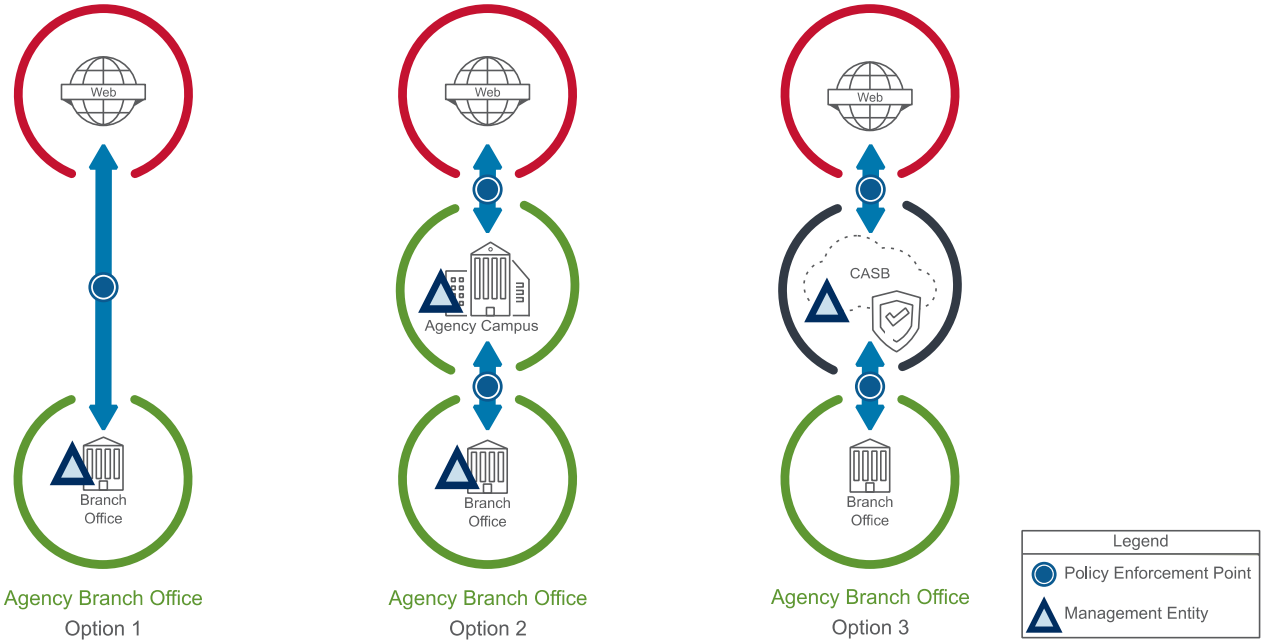

Figure 11: Example Security Pattern Implementation Options

5.2 Use Case Models

Use cases may be made up of multiple security patterns, each of which may have its own implementation options. The use case may include associated capabilities or implementation guidance for the security patterns or the common options for implementing those security capabilities. Figure 12 shows an example use-case for an agency branch office that communicates with the main agency campus, one or more CSP services, and the web.

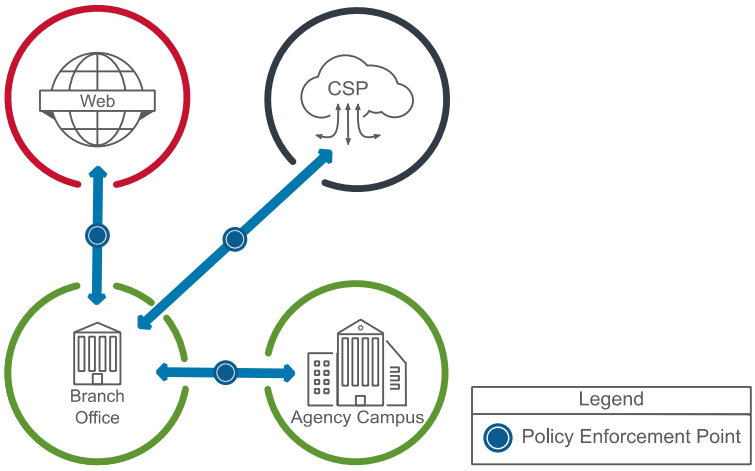

Figure 12: Example Use Case Diagram

An agency may construct its TIC architecture by combining multiple use cases. The implementation details for integrating the use cases will depend on the specific agency environment and are beyond the scope of the individual use case. Figure 13 shows an example diagram for an agency's TIC architecture, which combines two use cases: a traditional TIC use case for the agency campus access to the web and a branch office use case for traffic flow to and from the branch office.

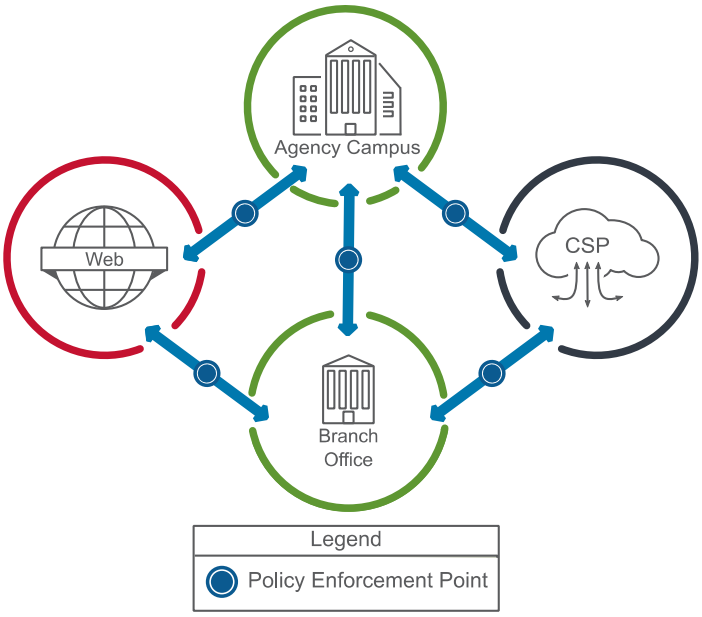

Figure 13: Example Agency TIC Architecture Diagram

6. Evolving from the Traditional Perimeter Architecture

The new concepts introduced above provide agencies with the flexibility to evolve from the traditional perimeter architecture if applicable. Traditionally, the TIC model was built around defending the network perimeter. In this model, as shown in Figure 14, there were two "trust zones," an internal zone and an external zone, with a single PEP, the TIC access point, where all TIC security protections are applied. From this perspective, all data flows to or from the external zone are untrusted and all data flows inside the internal zone are trusted.

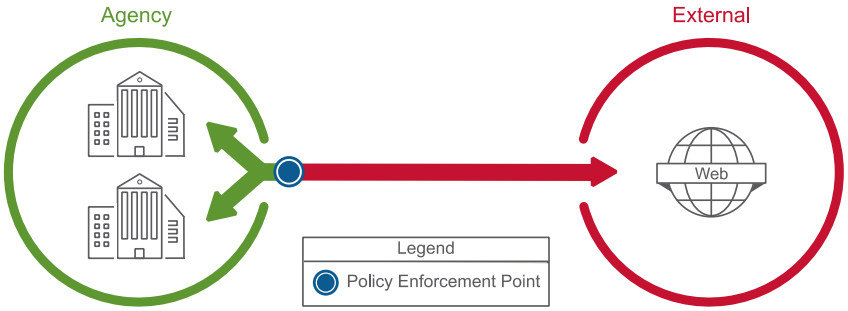

Figure 14: Traditional TIC Trust Zone Diagram

As agencies became more distributed, an agency's assets, data, and components became commonly located in areas beyond the agency's traditional network boundary, such as on remote devices, at cloud

data centers, and with external partners. To enable this model to continue working as agencies became more distributed, a common approach positioned the agency as a central hub between the distributed agency entities (e.g. branch offices, remote workers, cloud infrastructure) and entities in the external zone. Under this expanded model, shown in Figure 15, the distributed agency entities would be connected to the main agency campus, through methods like virtual private networks, with their traffic to the external zone routed through these connections.

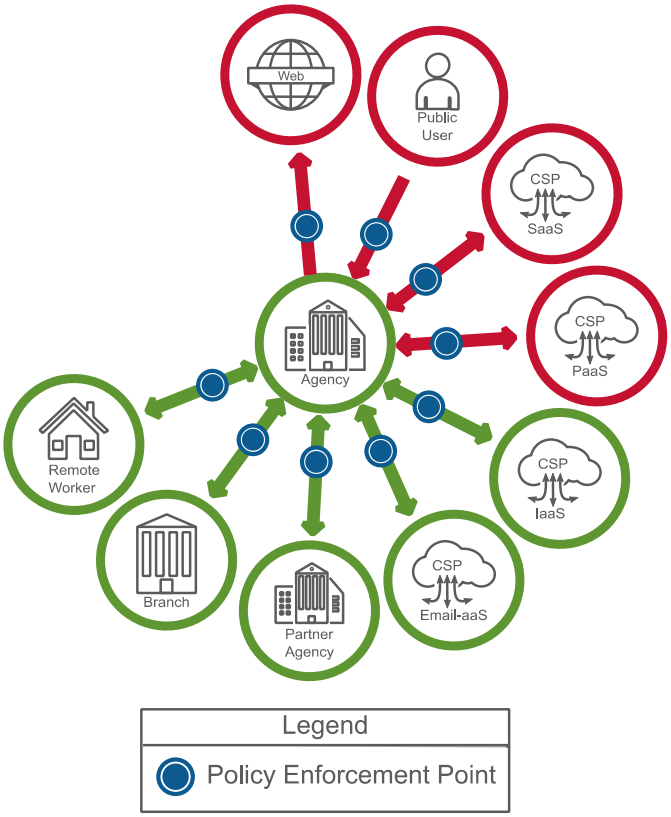

Figure 15: Traditional TIC Trust Zone Diagram for a Distributed Agency

6.1 A More Flexible TIC Model

While agencies are free to implement and use architectures adhering to a more traditional perimeter model, the IT infrastructure of federal agencies continues to evolve. Agency perimeters often no longer aligned with the strict internal-external boundary envisioned in the traditional model. It is common for agencies to utilize cloud services and accommodate remote workers' need access to all agency resources. These changes also impact the attack surface of the Federal Government. To facilitate this changing environment, TIC 3.0 allows for a more flexible perimeter definition. This enables a broader variety of current and future agency environments while maintaining a level of security commensurate with the threats faced by the Federal Government.

TIC 3.0 allows for distributing enforcement to different locations along the path if the deployed protections maintain a commensurate level of protection based on the agency's risk tolerance.

Instead of a singular location for policy enforcement, TIC 3.0 allows for distributing enforcement to different locations along the path if the deployed protections maintain a commensurate level of protection based on the agency's risk tolerance. Figure 16 shows an example of a trust zone diagram where an agency has deployed protections in a way that permits a remote worker to directly interact with a CSP without routing back through the protections on the main agency campus.

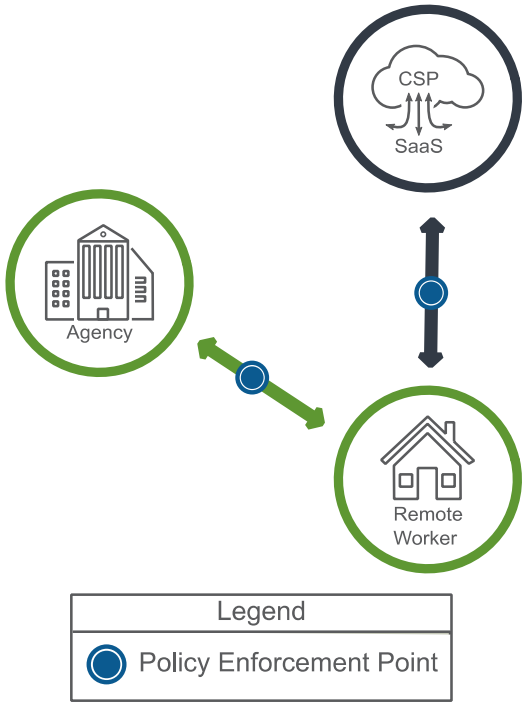

Figure 16: Distributed Policy Enforcement

While the example in Figure 16 defines the trust zones in a network-centric manner commonly employed in traditional perimeter defense, TIC 3.0 allows for trust zones to be defined independent of the underlying physical infrastructure. These logical trust zones enable the construction of more granular zones determined by agency criteria, like agency structures, application workflows, and identities, with trust zone boundaries protected by appropriate PEPs. Figure 17 shows a trust zone diagram based around an application workflow with each trust zone making up an individual component of the application's overall architecture.

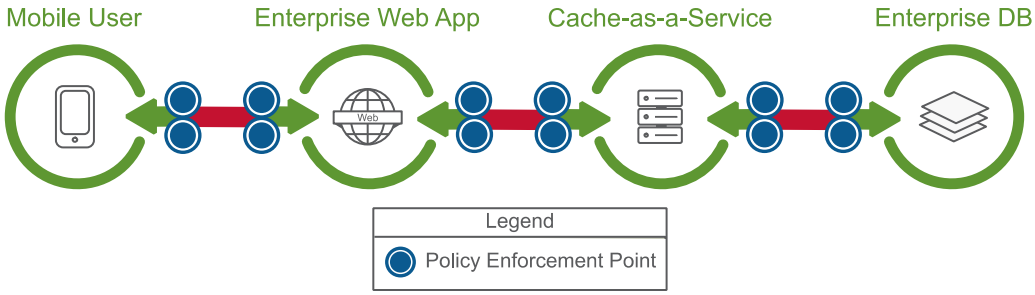

Figure 17: Logical Trust Zones

7. Conclusion

These building blocks allow agencies to explore modern architectures and new security approaches. The updated TIC initiative introduces new concepts that steer away from a one-size-fits-all approach. TIC concepts and solutions can be customized to fulfill agencies' unique security needs and to define evolving network architectures. This added flexibility provides federal agencies with more options in designing their networks or acquiring new information technology solutions. This reference architecture is a high-level technical document intended to provide federal agencies with the base information needed to implement TIC.

Stakeholders may leverage the Reference Architecture as a:

- Technical solutions foundational guide,
- Source of program common language and terminology, and
- Roadmap throughout the program implementation.

The key concepts and conceptual implementation of TIC 3.0 provide a solid technical foundation for the creation of individual TIC use cases. The concepts introduced in this document are expanded on when applied to the TIC use cases. Agencies are encouraged to implement TIC use cases in accordance with OMB M-19-26.

Appendix A – Glossary and Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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