Trusted Internet Connections 3.0

Vol. 2:

Reference Architecture

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Document Status

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

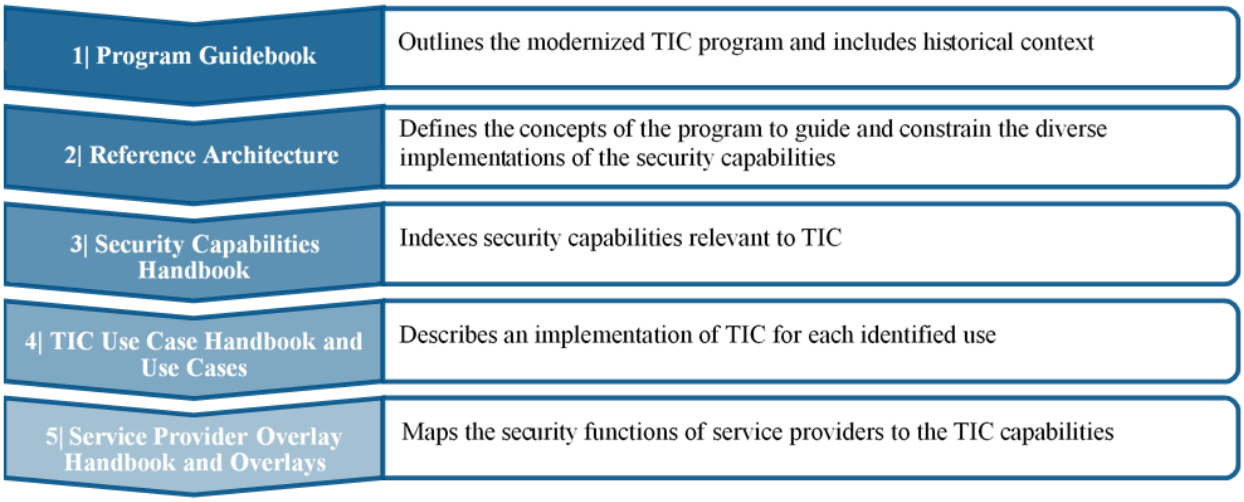
Disclaimer

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

Reader's Guide

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

Figure 1: TIC 3.0 Implementation Reader's Guide



TIC 3.0 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 perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative, setting requirements and an execution framework for agencies to implement a baseline perimeter or multi-boundary security standard.

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

1.1 Key Terms

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

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

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

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

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

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

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

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

Security Capability: Used to articulate security best practices and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means (i.e., functionality in hardware,

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

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

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

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

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

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

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

1.2 Updates and Changes

Historically, TIC has established and maintained a federal network security baseline by requiring agencies to consolidate and monitor their external network connections. The past iterations of the program focused on securing traffic at the physical agency network perimeter through a traditional TIC access point that operated EINSTEIN[2] sensors, deployed by the National Cybersecurity Protection System (NCPS) program. However, the federal IT landscape has shifted markedly in the decade since the TIC program's initiation, rendering this one-size-fits-all approach, in which all agency network traffic is routed through a limited number of agency-owned or service provider-maintained access points, increasingly unfeasible.

OMB Memorandum M-19-26 broadens the concepts of the program to accommodate cloud and mobile applications, services and environments. The program now envisions a flexible perimeter or multi-boundary as compared to the concept of a hard perimeter as previously conceptualized. While the NCPS and TIC initiatives continue to support and complement each other, the policy nor the program requires TIC access points and EINSTEIN sensors to be embedded into every type of architecture.

[2] "EINSTEIN," Cybersecurity and Infrastructure Security Agency (2019). https://www.cisa.gov/einstein.

2. Purpose of the Reference Architecture

The purpose of the Reference Architecture (hereafter announced as the "RA") is to be an authoritative source of information about TIC and provide high-level guidance on the application of the program, guiding the instantiations of the TIC Use Cases. The RA can be leverage to:

- Serve as a reference 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. Strategic Program Goals

In accordance with the *IT Modernization Report*, CISA, in coordination with OMB and GSA, developed seven strategic goals to guide the TIC modernization effort. These goals are the guideposts for TIC 3.0, outlining the approach to securing dispersed network environments across the federal civilian enterprise to include service providers hosting federal systems and information in the cloud. These goals are reflected in all documentation and requirements associated with the program.

1. Boundary-Focused

As the Federal Government continues to expand into cloud and mobile environments, systems and assets will increasingly be dispersed which will require TIC capabilities to support diverse security services and implementation approaches. TIC 3.0 adopts a flexible framework to address and support advanced security measures across branch offices, remote users, cloud and other service providers, mobile devices, etc. These additional network boundaries require different placement and roles of security capabilities than those employed to protect the enterprise perimeters of federal agencies. TIC 3.0 divides agency architectures by trust zones, shifting the emphasis from a strictly physical network perimeter to the boundaries of each zone within an agency environment to ensure baseline security protections across dispersed network environments. This shift in approach from securing a single network boundary to a distributed architecture is the most fundamental change from the legacy TIC program.

2. Descriptive, Not Prescriptive

The past iterations of the program focused on securing traffic at the physical agency network perimeter through a limited number of secured access points. With advances in technology, the federal IT landscape has shifted markedly since the TIC program's initiation in 2007, rendering this one-size-fits-all approach inflexible and counterproductive to meet the demands to modernize and move to cloud. The updated reference architecture, taxonomy, capabilities, and use cases will broaden the concepts of the program to accommodate cloud, mobile, and encrypted applications, services and environments. These documents will provide guidance to agencies to implement TIC in a manner that best suits their needs.

3. Risk-Based to Accommodate Varying Risk Tolerances

Federal agencies have varying degrees of risk tolerances that must be considered as IT modernization tasks are planned and executed. Agencies must consider the security capabilities that are necessary to secure TIC environments. In some cases, the controls identified in the TIC 3.0 documentation may not provide enough security to adequately address residual risks necessary to protect information and systems. In cases where additional controls are necessary to manage residual risk, agencies are obligated

to apply the controls or explore options for compensating controls that achieve the same protections to manage risks. TIC 3.0 leverages cloud and other service providers to develop and maintain security control overlays to assist agencies with identifying service provider capabilities that can be applied to secure their environments. To the extent practical, agencies are encouraged to leverage existing enterprise capabilities capable of providing protections for on-premise or service provider hosting environments, to include those provided by the CDM.

4. Environment-Agnostic

Every agency operates with unique missions, business needs, resource availability, and risk tolerances. To maximize the applicability of TIC guidance, the terms, definitions, and logical components of network infrastructure and solutions are vendor and technology-neutral. Additionally, the modernized TIC provides flexibility on the application of the security capabilities to accommodate a variety of agency environments; these are captured in the TIC Use Cases.

5. Dynamic and Readily Adaptable

To keep pace with technological innovation, the TIC Program Management Office (PMO) will continue to produce and update use cases and overlays through collaboration with agencies and service providers to maintain currency. The TIC PMO will also update core guidance, reference architectures, and capabilities based on agency and public feedback, evolving threats, and emerging cybersecurity trends.

6. Automated and Streamlined Verification

In accordance with the IT Modernization Report, the modernized TIC initiative eliminates the existing TIC-related FISMA metrics and manual TIC Compliance Validation (TCV) process, replacing both with automated metric collection as applicable. The primary focus of the validation is security and availability measures. The validation will leverage existing capabilities under the CDM program. The program's goal is to define scalable, comprehensive and continuous validation processes for ensuring agency implementation of TIC capabilities in contrast to the point-in-time reviews.

7. Delineate the NCPS and TIC Initiatives

CISA continues to provide these security capabilities in accordance with the *Federal Cybersecurity Enhancement Act of 2015* to protect "all information traveling between an agency information system and any information system other than an agency information system." The NCPS EINSTEIN and TIC initiatives will continue to support and complement each other in support of this legislation. The NCPS PMO and TIC PMO will independently provide guidance for their respective initiatives. Additional information regarding the relationship between the TIC and NCPS initiatives can be found in the TIC 3.0 Program Guidebook.

4. Summary of Key Program Documents

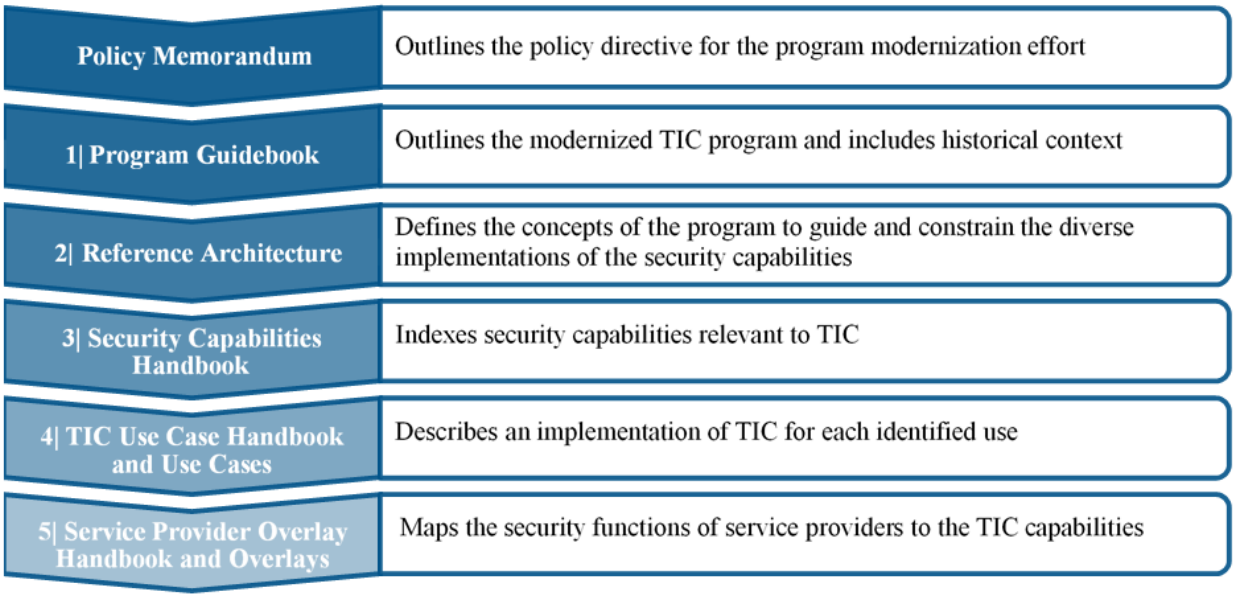
The TIC 3.0 guidance documentation, listed in Figure 2, is intended to be used collectively in order to achieve the goals of the program. The TIC policy memorandum, OMB Memorandum M-19-26, lays the foundation for the program, outlining the expectations for TIC to:

- Provide flexibilities necessary for modern architectures,
- Remove barriers to cloud adoption, and
- Establish a process that promotes continuous review and updates to the TIC initiative.

CISA is responsible for translating the expectations, outlined in OMB Memorandum M-19-26, into technical guidance through the subsequent four documents. The TIC 3.0 Program Guidebook explains the need to modernize the TIC program, providing historical context and the modernization approach. The RA builds on the program guidebook, detailing the key concepts of the program to guide and constrain the instantiations of the use cases. Complementary to the RA, the TIC 3.0 Security Capabilities Handbook features an index of security capabilities applicable to TIC 3.0.

The RA and the TIC 3.0 Security Capabilities Handbook create the foundation for the use cases. The use cases provide guidance on the secure implementation and/or configuration of specific applications, services, and environments by applying applicable security capabilities. TIC Use Cases are a mechanism to accommodate the secure use of cloud and mobile environments in the Federal Government. All key documents will be refreshed to reflect changes in the technological landscape, strategic priorities and feedback from agencies and industry.

Figure 2: TIC 3.0 Key Program Documents List



5. 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 intent of the objectives is to limit the potential impact of a cybersecurity event. Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected. The objectives are described in Table 1 below; all references to traffic are notional, describing data, connections, etc.

Table 1: TIC 3.0 Security Objectives

Objective	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

The TIC Security Objectives should be viewed independently of the types of traffic being secured, but different types of traffic will 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 in order to execute another.

6. Key Concepts of TIC 3.0

The implementation of the objectives and subsequent capabilities are guided and constrained by the key concepts. The concepts are intentionally abstract to ensure the program can be applied across a multitude of platforms, services, and environments. Trust zone diagrams encapsulate each of the four key concepts to provide context for the implementation of the capabilities:

- Trust Zones,
- Policy Enforcement Points (PEPs),
- Management Entities (MGMT), and
- Security Capabilities.

6.1 Trust Zones

Whereas previous versions of TIC focused on an environment where there was a single boundary between an agency and the Internet, this version addresses agencies' distributed networks to include branch offices, remote users and service providers (SP). These additional network boundaries require different placement and roles of security capabilities which divides agency architectures by trust zones.

A trust zone is a discrete computing environment involved in information processing, storage and/or transmission that dictates the rigor or robustness of the applicable security capabilities necessary to protect the zone. The trust level is designated from the agency's perspective, it is based on the control, transparency, sensitivity, and verification of the data. Agencies can use any gradient for designating differences in trust zones. To illustrate the concept, the RA uses three levels of different trust zones: high, medium, and low trust zones. These three levels, depicted in Figure 3, should only be considered an example of how an agency can designate different trust zones. Agencies can use the categorization or gradient scheme most appropriate for their environment. For example, an agency could have eight categories of trust versus the three depicted in Figure 3. The criteria for designating trust zones are detailed in Section 8.1.1.

Figure 3: Example Trust Zone Gradient

This trust zone concept is in line with the concepts of Zero Trust. A trust zone must adhere to the security outcomes as identified or described in the use case. A trust zone does not always inherit trust/security from an adjacent trust zone, nor does the trust and the subsequent security capabilities depend on the trust of the adjacent zone.

6.1.1 Trust Zone Criteria

Once the zones are identified from the logical architecture, each zone can be assigned a specific trust designation. Following the three-trust zone example gradient, and applying to the TIC 2.0 architecture, the "Agency's Enterprise Network" can be considered a high trust zone. The "Internet" is typically considered a low trust zone. TIC 3.0 accounts for the varying degrees of security requirements introduced following the federal adoption of cloud services.

Depicted in Table 2, the trust criteria give agencies a framework to determine the trust zones within their environment, enabling them to effectively implement TIC capabilities. Table 2 provides the criteria for defining the trust level of a zone (e.g., high, medium or low) based on an agency's:

- the level of control,
- the level of transparency,
- the level of verification, and
- the sensitivity of the data within the environment.

Table 2: TIC 3.0 Trust Criteria

TRUST CRITERIA	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 environment's compliance with relevant controls, standards and/or best practices?	An agency is ***able to continuously validate*** the environment's compliance (e.g., through continuously-collected data or APIs).	An agency is ***able to periodically validate*** *the* environment's compliance (e.g., through annual audit).	An agency ***does not have access to information*** validating the environment's compliance.
Data Sensitivity: Consider the impact of compromise to an agency's information system's confidentiality, integrity or availability.	An agency follows its internal agency and applicable federal guidance for defining high data sensitivity (e.g., an agency's information system ***does contain a high value asset (HVA))***.	An agency follows its internal agency and applicable federal guidance for defining medium and/or moderate data sensitivity.	An agency follows its internal agency and applicable federal guidance for defining low data sensitivity (e.g., an agency's information system ***does not contain HVA)***.
Agency Specific: An agency may be constrained by additional requirements such as legislation, compliance regulations, etc.	An agency follows the guidance to meet additional high trust requirements as necessary.	An agency follows the guidance to meet additional medium trust requirements as necessary.	An agency follows the guidance to meet additional low trust requirements as necessary.

The trust criteria give agencies the flexibility to also incorporate unique variables (e.g., HVA requirements, FISMA, Risk Management Framework[3], etc.) into their trust determinations.

Agencies should use the trust criteria to determine the appropriate trust level of the zones within their environment proportional to the risk of the zone being protected. As outlined, agencies are responsible for protecting all trust zones at a level commensurate with the designated trust.

Figure 4 below highlights that a single environment can have a different trust designation depending on the scenario. For example, an agency may classify SPs as a high, medium or low trust zone depending on the criteria outlined in Table 2. An agency could also categorize one SP as a medium trust zone and another as a low trust zone based on various circumstances, like the presence of personally identifiable information or stronger contractual terms that provide greater visibility into the SP.

Figure 4: Trust Zone Examples

6.2 Policy Enforcement Points (PEPs)

In past iterations of the TIC program, the PEPs were the TIC access points used to secure the agency network boundary. They were controlled by a TIC Access Provider (TICAP) or an approved Multi-Service TICAP. The PEPs are now intentionally abstract to account for additional PEPs associated with cloud service providers.

In this latest iteration, the PEPs are used to secure trust zones managed, or in any way controlled, by an agency (e.g., cloud service providers). The PEPs can be security devices, tools, functions or applications that enforce security capabilities associated with TIC. An individual PEP may enforce all of the security capabilities associated with a given trust zone. Some PEPs may only meet a subset of the applicable security capabilities and can be combined with complimentary PEPs to meet all capabilities.

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

6.3 Management Entities (MGMT)

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

- organizations (e.g., NOC/SOCs, 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 information such as alerts, system inventories, and capability status.

6.4 Security Capabilities

The security capabilities listed in the TIC 3.0 Security Capabilities Handbook define the baseline security capabilities foundational to the TIC initiative. NIST defines a security capability as a combination of mutually reinforcing security controls (i.e., safeguards and countermeasures) 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.

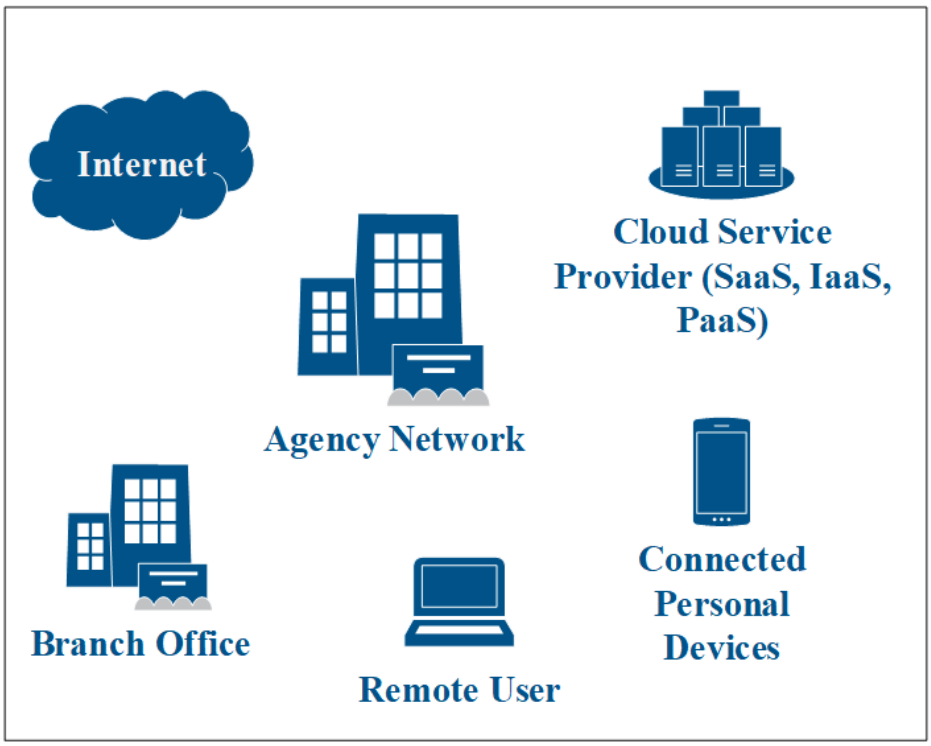
The capabilities assigned to each use case are focused and scoped by the TIC security objectives in Table 1. Capabilities can support multiple objectives or be assigned to a particular objective as most relevant, depending on the circumstances.

[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.

7. Conceptual Implementation of the TIC 3.0

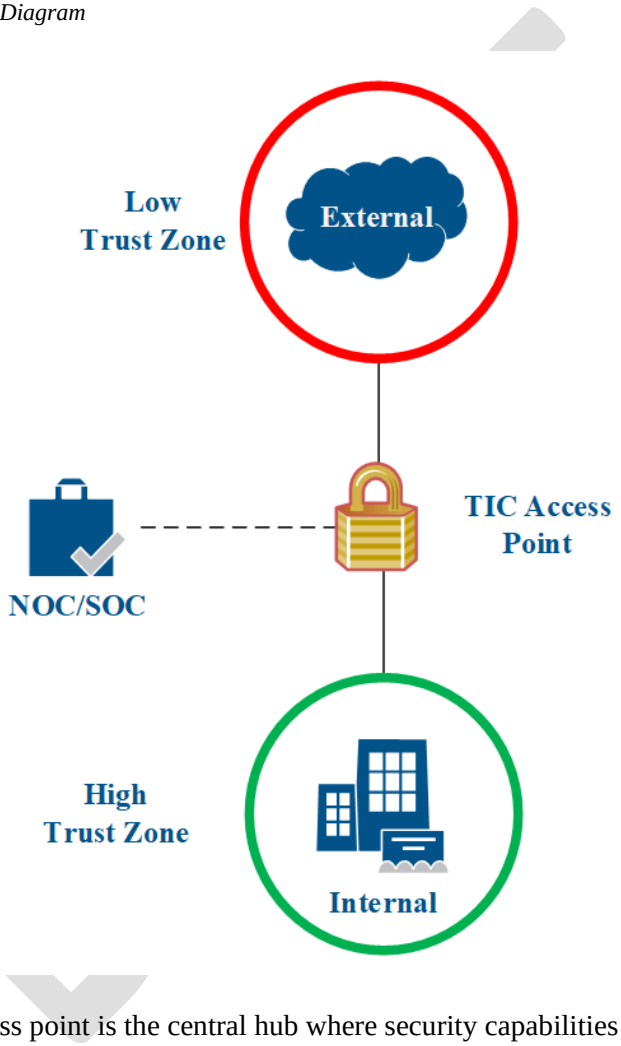
As the Federal Government expands into the cloud, an agency's assets, data, and components are commonly located in areas beyond the agency's network boundary, such as on remote devices, at cloud data centers, with external partners, etc. The generalized architecture in Figure 5 emphasizes the distributed nature of the agency network. The RA intends to promote flexibility for the broad variety of current and future agency environments, while maintaining a level of security commensurate with the threats faced by the Federal Government.

Figure 5: General Agency Network Components



While the distributed network is not unique to TIC, previous iterations implemented security by consolidating the network into two main trust zones: Internal/Agency Zone and External Zone. Version 2.0 simplified the environment to a single, large boundary between an agency and external networks, including the Internet. At that boundary, TIC access points are deployed by a TICAP or a MTIPS. Agency traffic flows through an access point that contains all of the security capabilities outlined in TIC 2.0. The trust zones in version 2.0 emphasize the reduction in control that agencies have over their data when it leaves the network perimeter. Figure 6 depicts the consolidated security configuration laid out in version 2.0.

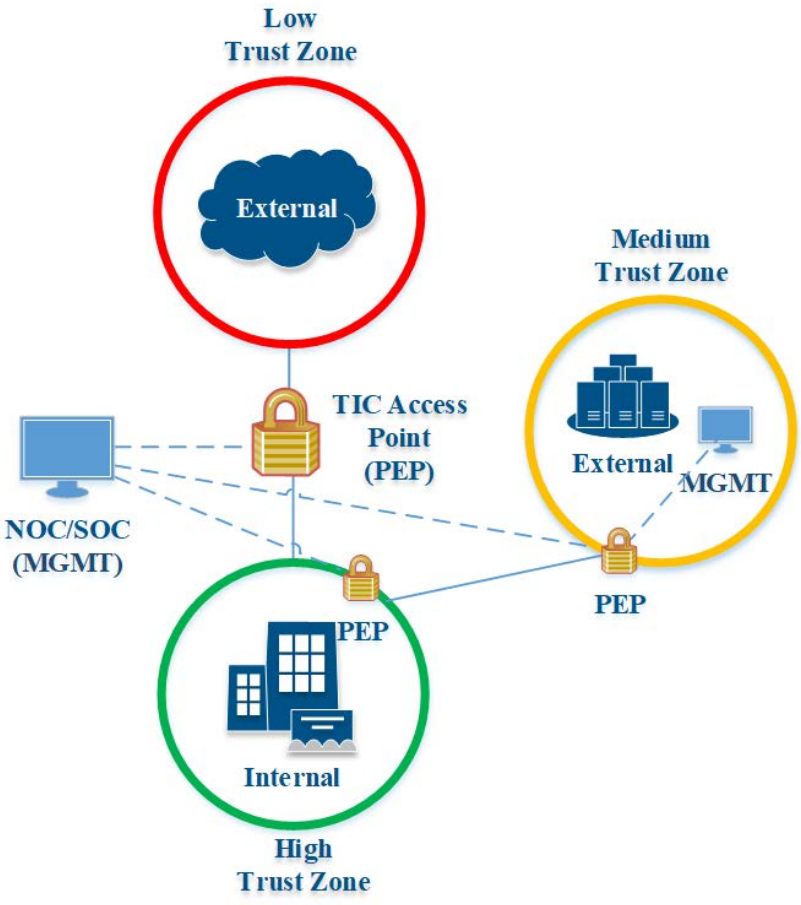
Figure 6: TIC 2.0 Trust Zone Diagram



In TIC 2.0, the TIC access point is the central hub where security capabilities are implemented. The TIC access point includes firewalls, CISA's sensors, intrusion detection and prevention systems, web application firewalls, data loss prevention software, etc. This security configuration, while promoting high-levels of security, can have significant implications on operational and fiscal efficiency as all of the agency's external traffic must flow through this access point.

In version 3.0, this concept is expanded to allow flexibility in the implementation of security capabilities to increase efficacy and efficiency for agencies. The inclusion of medium trust zones, PEPs, and MGMT give agencies the autonomy to implement security capabilities in the most effective manner for their architecture. Figure 7 depicts the configuration of TIC 2.0 within the more flexible conceptual implementation of TIC 3.0.

Figure 7: TIC 3.0 Trust Zone Diagram



The configuration depicted in Figure 7 gives agencies the flexibility to implement security capabilities closer to the agency's data in the different trust zones. By applying security capabilities throughout their environment, agencies will have greater visibility into their network, leading to increases in operational and fiscal efficiencies.

8. Conclusion

The updated TIC initiative introduces new concepts that steer away from a one-size-fits-all approach. This comprehensive solution can be customized to fulfill agencies' unique security needs and evolving network architecture. This added flexibility provides federal agencies with more options in designing their networks or acquiring new information technology solutions. The RA is a high-level technical document intended to provide federal agencies with the information needed to navigate through the process of implementing the program. Stakeholders may leverage the RA as a:

- Technical solutions foundation guide
- Source of program common language and terminology
- Roadmap throughout the program implementation

The key concepts introduce a solid technical foundation that provides a baseline for TIC Use Cases. Agencies are encouraged to implement the TIC Use Cases in accordance with OMB Memorandum M-19-26. The proper implementation of TIC promotes secure network traffic within the federal enterprise trust zones and expands into all agency traffic, including cloud communications.

Appendix A – Definitions, Acronyms, and Attributions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Security Capability: Used to satisfy the security requirements and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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