CISA
CYBER+INFRASTRUCTURE

Trusted Internet Connections 3.0

Traditional TIC Use Case

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Draft

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.

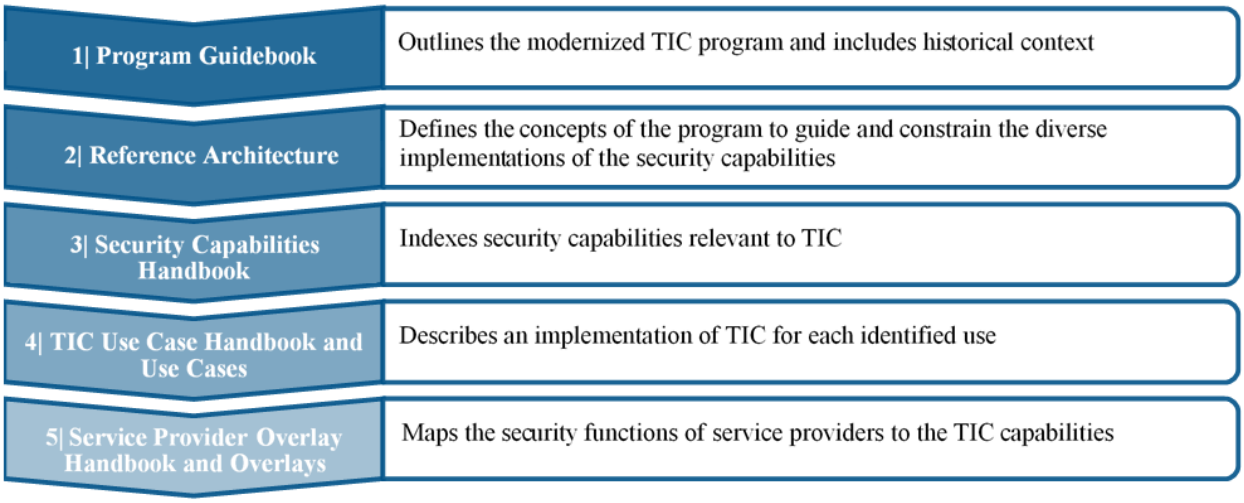
Disclaimer

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 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, 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 PEPs, and it allows IT professionals to control devices on the network.

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

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

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

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

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

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

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

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

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

2. Purpose

TIC Use Cases are intended to describe the current state challenges, limitations, characteristics, scope of the technology need, and target state of TIC architectures and implementations. The use cases provide sufficient details to clearly articulate the goals and objectives of a given technology or service in support of agency modernization efforts, including:

- Planning – Scope, schedule, resources, risks, assumptions;
- Acquisitions – Key requirements, market research;
- Implementation – Green field or migration of existing system;
- Diagrams – Data flow, transport, key security, monitoring services and capabilities, and PEPs (PEPs); and
- Technical Analysis – Critical/key questions that need to be answered, measurement/metrics.

Use cases are supported by other artifacts, including:

- TIC 3.0 guidance documentation,
- Use case proposals,
- Project plans,
- Requirement plans,
- Capability documentation (agency and vendors),
- Technical diagrams,
- Security guidance and control overlays, and
- Requirements traceability matrices.

Over time, for a given use case, there may be more than one set of supporting artifacts based on differing operational characteristics and development of capabilities provided by service providers.

3. Traditional TIC Use Case

The Traditional TIC Use Case defines how network security should be applied when an agency has personnel in one physical location, an agency campus, and seeks to connect to the Web for both general web services as well as to a trusted external partner. A trusted external partner may include a sanctioned cloud service provider (CSP) if no other use case is used, another agency, or a trusted web-based service, among others. When an agency is connecting to an external partner, it is responsible for vetting the partner and ensuring appropriate data protections are in place.

The two network traffic flows that need to be considered in this TIC use case include:

- Secure agency campus access to Web
- Secure agency campus access to an external partner

An agency may implement a subset of these traffic flows and not necessarily both. For instance, an agency may not yet have sanctioned cloud services to which it had authorized direct connectivity from the agency campus.

The Traditional TIC Use Case is backward compatible with TIC 2.0 protections that are in place at an agency TIC Access Point or a Managed Trusted Internet Protocol Services (MTIPS) solution.

3.1 Assumptions and Constraints

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.
- The TIC capabilities applicable to the use case are not dependent on a data transfer mechanism. In other words, the same 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.

- Data is protected commensurate to what the agency has determined.
- 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, a cloud access security broker (CASB), or commensurate solutions.

The following are assumptions about the external partner.

- Interaction with external partners will 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 the external partner or permits the external partner access to only limited and well-defined services of the agency.
- The agency uses services of the external partner or provides services to the external partner that are web-based (e.g. site-to-site VPN, remote access, and multi-protocol like secure file transfer protocol (SFTP), simple mail transfer protocol (SMTP), etc.) are beyond the scope of this use case.
- The external partner has a NOC and SOC that controls and protects the portions of the service infrastructure where the agency has little to no control or visibility.

- The agency only communicates over secure mechanisms (e.g. multifactor authentication (MFA), transport layer security (TLS), etc.) with the external partner.
- Data at the external partner is protected commensurate to what the agency has determined.

The following are assumptions about the Web:

- The Web contains untrusted users.
- The agency has no ability to apply policy in the Web.

3.2 Conceptual Architecture

As shown in Figure 2, the Traditional TIC Use Case is composed of three trust zones: agency campus, Web, and external partner. Agency network traffic moves to and from the open Web and to and from an external partner. Table 1 describes the components in this security pattern.

Figure 2: Traditional TIC Security Pattern

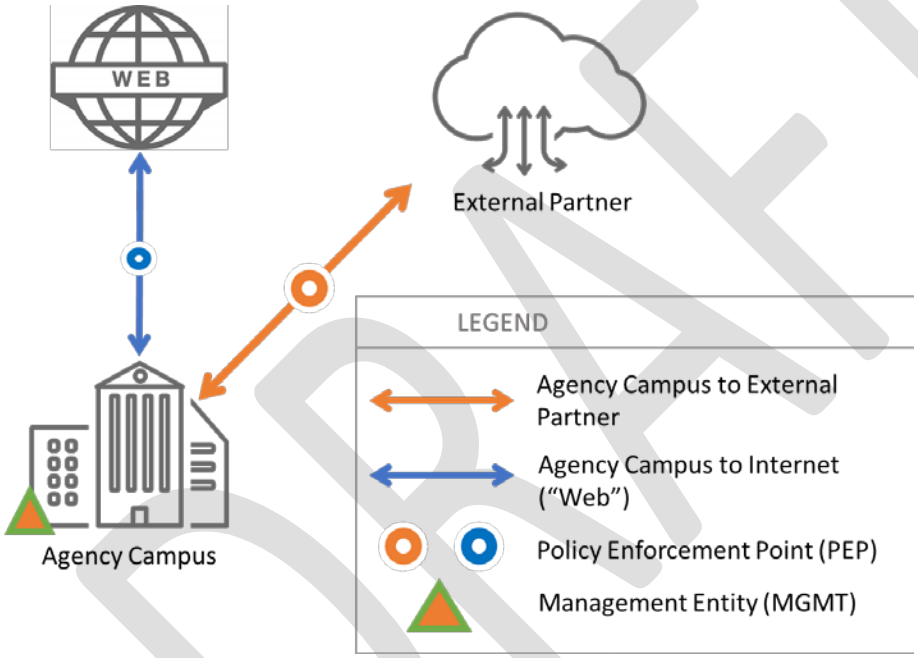


Table 1: Components of the Traditional TIC Security Pattern

Component	Description
Agency Campus	The agency campus or the agency's enterprise network trust zone. Includes a MGMT entity such as the NOC and SOC and other entities for the agency responsible for defining policies, implementing them in the various PEPs controlled by the agency, and searching for and responding to incidents. This is managed by the agency. This point includes various controls associated with establishing a trusted connection to and from the Web and CSPs.
Web	An environment with untrusted external users, and with no PEPs or MGMT entities where the agency, or entities acting on its behalf, may deploy policies.
External Partner	The external partner providing a web-based service trust zone. The external partner is responsible for protecting the underlying service infrastructure with certain defined functions/capabilities managed in accordance with agency and external partner agreements. In addition, the policy enforcement point between the external partner and the agency. This point is a shared responsibility deployment model with the external partner and agency implementing mutually agreed-upon policies for information exchange.

3.3 TIC Security Capabilities: Universal Security Capabilities

The TIC 3.0 Security Capabilities Handbook contains a table of Universal Security Capabilities that apply across use cases. The agency can determine the level of rigor that is applied to these Universal Security Capabilities such that it is in line with the agency risk tolerance and federal guidelines. Unique guidance for applying some of these Universal Security Capabilities in the Traditional TIC Use Case are outlined in Table 2.

Table 2: Guidance on Applying Universal Security Capabilities in the Traditional TIC Use Case

Capability	Use Case Guidance
Backup and Recovery	The agency must ensure access to restoration configuration and data is readily available.
Central Log Management with Analysis	The agency may select to host centralized log services on-prem or at a sanctioned cloud location.
Resilience	The agency must consider their availability, compliance, cost, and administration requirements as well as risk tolerance when deciding on the scope of redundant resources.
Enterprise Threat Intelligence	Threat intelligence may be delivered utilizing one of two mechanisms, either through a local cache with a full repository, or a remote lookup on demand through API interactions. On-prem caches may need to make themselves available for additional agency PEP utilization. Centralized administration of threat intelligence can aide in licensing and vendor compliance enforcement.

3.4 TIC Security Capabilities: Policy Enforcement Point Capabilities

As shown in Figure 2, there are PEPs on all three data flows: branch office to agency campus, branch office to CSP, and branch office to Web. The application of specific PEP Capabilities to these data flows will be discussed in each of the security patterns in the next section. The following table provides high-level guidance on what PEP Capability groups will be applied in the Traditional TIC Use Case.

Table 3: General Guidance on PEP Capability Groups in the Traditional TIC Use Case

PEP Capability Group	**Inclusion Justification**
Files	Agency users and services may utilize file transfers as part of their information exchanges.
Web	Agency users and services may use external Web services.
DNS	Agency users and services will use DNS services. The agency may also be hosting authoritative name services for their domain names.
Intrusion Detection	Agencies will be providing security services for their users, services and data flows
Enterprise	Agencies will be security their enterprise networks.

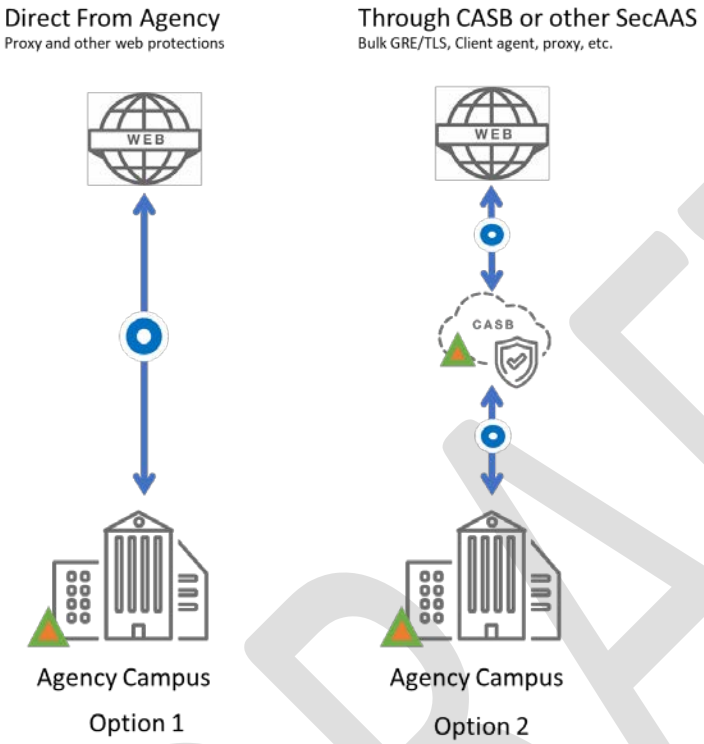
3.5 Security Patterns

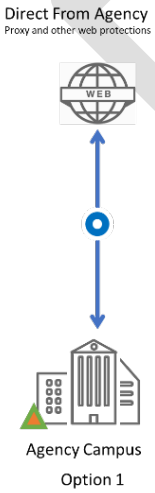
Two security patterns capture the data flows for the agency Traditional TIC Use Case. Each of these has distinct sources, destinations, and options for policy enforcement. Regardless of the options chosen, due diligence must be practiced ensuring agencies are protecting their information in line with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

3.5.1 Traditional TIC Security Pattern 1: Agency to Web

Figure 3 illustrates the Traditional TIC Security Pattern 1 where an agency has connections to the open internet for web services. Connections in this security pattern are the riskiest, as there is a connection from the agency to the untrusted Web. There are two options for this connectivity. This will require the greatest amount of rigor to be applied to capabilities in place in the Agency PEP.

Figure 3: Security Pattern 1: Agency to Web





Option 1 depicts a direct connection from the agency campus to the Web for user web connections. The Agency PEP ensures traffic is forwarded to the Web and all applicable security policies are enforced. Care must be taken by the agency to ensure the same protections are applied to all traffic destined for the Web, regardless of origin.

Option 2 depicts a connection from the agency campus to the Web for user web connections, utilizing a CASB or other Security As A Service (SecAAS) provider as an intermediary traffic forwarding step. The agency PEP ensures traffic is forwarded to the CASB with appropriate connection security. The CASB PEP ensures both connection security to the agency and all applicable security policies are enforced for connections destined for the Web. Care must be taken to ensure the same protections are applied to all traffic destined for the Web, regardless of origin.

The PEP Capabilities in Table 4 are applied to Traditional TIC Security Pattern 1. The agency can determine the level of rigor that is applied to these capabilities such that it is in line with the agency risk tolerance and federal guidelines.

Table 4: Traditional TIC Security Pattern 1: TIC PEP Capabilities

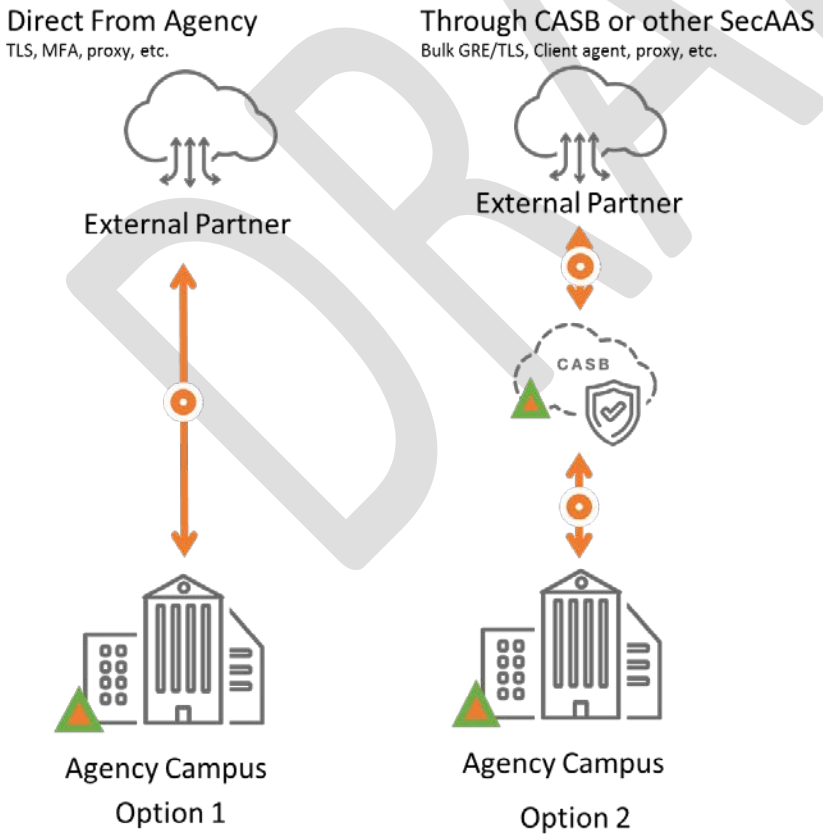
PEP Capability Group	**PEP Capability**
Files	Anti-malware
	Content Disarm & Reconstruction
	Detonation Chamber
Web	Break and Inspect
	Active Content Mitigation
	Certificate Blacklisting
	Certificate Consensus
	Content Filtering
	Authenticated Proxy
	Data Loss Prevention
	DNS-over-HTTPS Filtering
	RFC Compliance Enforcement
	Domain Category Filtering
	Domain Reputation Filter
	Bandwidth Control
	Malicious Content Filtering
	Access Control

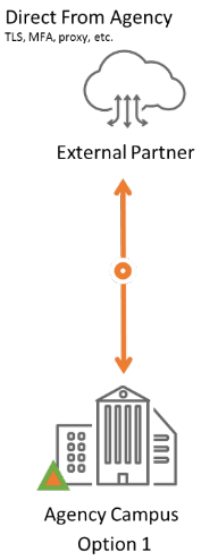
DNS	DNS Blackholing
	DNSSEC for Agency Clients
	DNSSEC for Agency Domains
Intrusion Detection	Endpoint Detection and Response
	Intrusion Protection System
	Adaptive Access Control
	Deception Platforms
	Certificate Transparency Log Monitoring
Enterprise	Security Orchestration, Automation, and Response
	Shadow IT Detection

3.5.2 Traditional TIC Security Pattern 2: Agency to External Partners

Figure 4 illustrates connections where an agency is utilizing web services of an external partner or is providing web services to an external partner. This communication can take place through two options, outlined below. Regardless of the option chosen, due diligence must be practiced ensuring Agencies are protecting their information in line with their risk tolerances.

Figure 4: Security Pattern 2: Agency to External Partner





Option 1 consists of a direct connection from the agency campus to the external partner. The Agency PEP hosts the components which will ensure proper traffic forwarding, protections, and eligibility enforcement for external partners vs. non-partner destinations for agency traffic. The Agency PEP will ensure that data flows to and from external partners are properly protected and only authorized services and information are being exchanged.

Option 2 consists of a connection from the agency campus to the external partner, utilizing a CASB or other SecAAS provider as an intermediary forwarding step. The Agency PEP hosts the components which will ensure proper traffic forwarding and protections for all traffic to the CASB. The CASB PEP ensures eligibility enforcement for external partner versus non-partner destinations for agency traffic. The Agency PEP or the CASB PEP will ensure connections for data flows are properly protected and only authorized services and information is being exchanged with the external partner.

The PEP Capabilities in Table 5 are applied to Traditional TIC Security Pattern 2. The agency can determine the level of rigor that is applied to these capabilities such that it is in line with the agency risk tolerance and federal guidelines.

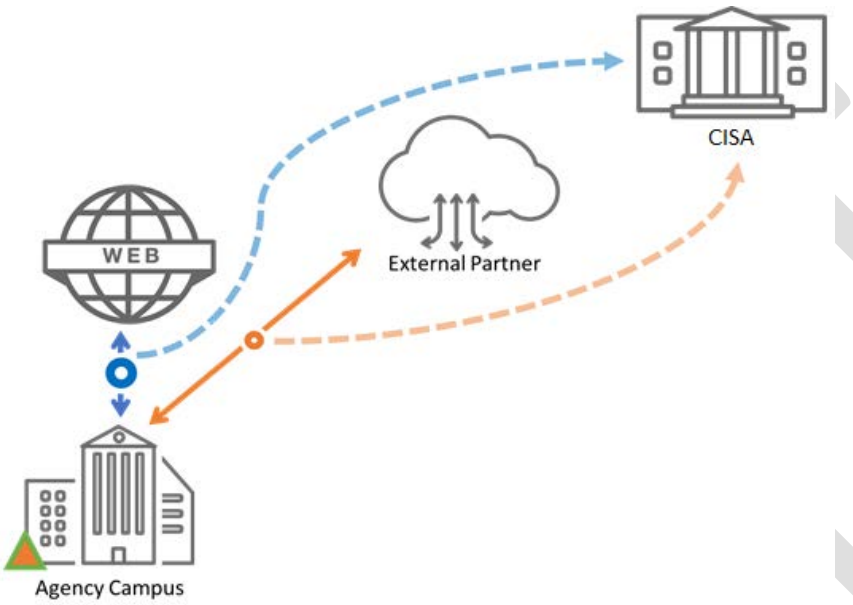
Table 5: Traditional TIC Security Pattern 2: PEP Capabilities

PEP Capability Group	**PEP Capability**
Files	Anti-malware
	Content Disarm & Reconstruction
	Detonation Chamber
Web	Break and Inspect
	Active Content Mitigation
	Certificate Blacklisting
	Certificate Consensus
	Content Filtering
	Authenticated Proxy
	Data Loss Prevention
	DNS-over-HTTPS Filtering
	RFC Compliance Enforcement
	Domain Category Filtering
	Domain Reputation Filter
	Bandwidth Control
	Malicious Content Filtering
	Access Control
DNS	DNS Blackholing
	DNSSEC for Agency Clients
	DNSSEC for Agency Domains
Intrusion Detection	Endpoint Detection and Response
	Intrusion Protection System
	Adaptive Access Control
	Deception Platforms
	Certificate Transparency Log Monitoring
Enterprise	Security Orchestration, Automation, and Response
	Shadow IT Detection

3.6 Telemetry Requirements - Information Sharing with CISA

As agencies transition away from traditional NCPS, visibility by CISA must be preserved through information sharing. Figure 5 shows the conceptual architecture of the Traditional TIC Use Case with the telemetry requirements added as dashed lines on certain data flows. These dashed lines indicate when an agency must share telemetry with CISA.

Figure 5: Traditional TIC Telemetry Sharing with CISA



4. Conclusion

This document provides guidance on how an agency can configure its Traditional TIC data flows and apply relevant TIC security capabilities. This use case document should be used in conjunction with the TIC 3.0 Security Capabilities Handbook and other TIC 3.0 guidance documentation.

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.