Trusted Internet Connections 3.0

Branch Office 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.

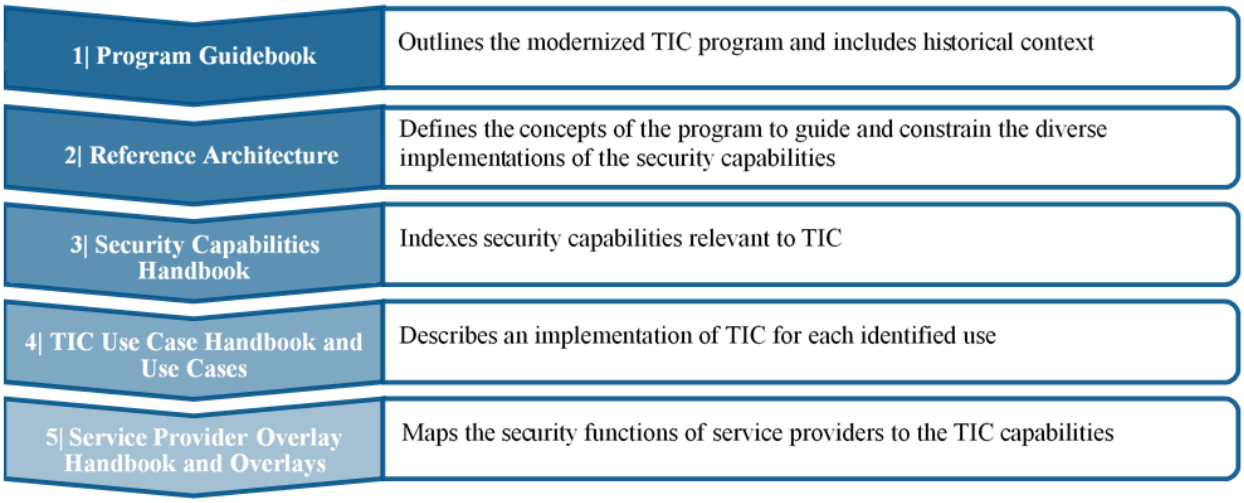
Disclaimer

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 Branch Office 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 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.

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 policy enforcement points (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. Branch Office Use Case

The Branch Office Use Case defines how network and multi-boundary security should be applied when an agency has personnel in more than one physical location. This use case helps agencies gain application performance (latency, throughput, jitter, etc.); reduce costs (through reduction of private links); and improve user experience by facilitating branch office connections to agency-sanctioned cloud services, the Web, and agency internal services. The TIC 3.0 Traditional TIC Use Case enumerates the TIC protections for agency campus and will not be repeated here.

This use case considers three network security patterns:

- Secure branch office access to a sanctioned cloud service provider (CSP),
- Secure branch office access to the Web, and
- Secure branch office access to the agency campus.

An agency may implement a subset of these security patterns and not necessarily all three. For instance, an agency may not yet have sanctioned cloud services to which it had authorized direct connectivity from a branch office location. In that case, the agency may only implement the branch office to Web and branch office to agency campus security patterns.

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 branch office.

- Data is protected commensurate to what the agency has determined.
- A NOC and SOC function exists at the branch office as an extension to the NOC and SOC tools managed and housed at the agency.

The following are assumptions about the CSP.

- The CSP is compliant with the Federal Risk and Authorization Management Program (FedRAMP)[2].
- The CSP has a NOC and SOC that controls and protects the portions of the service infrastructure where the agency has little or no control or visibility.
- Data at the CSP is protected commensurate to what the agency has determined.
- The CSP allows the agency to define or configure policies that the agency applies on behalf of the agency and allows the agency to define roles and responsibilities for the configuration of those policies.
- The CSP provides the agency with mechanisms for obtaining visibility into the current state and history of the system (e.g., log information).
- The CSP provides the same protections and policy enforcement for traffic between the agency and other tenants of the CSP as between the agency and parties outside the CSP.

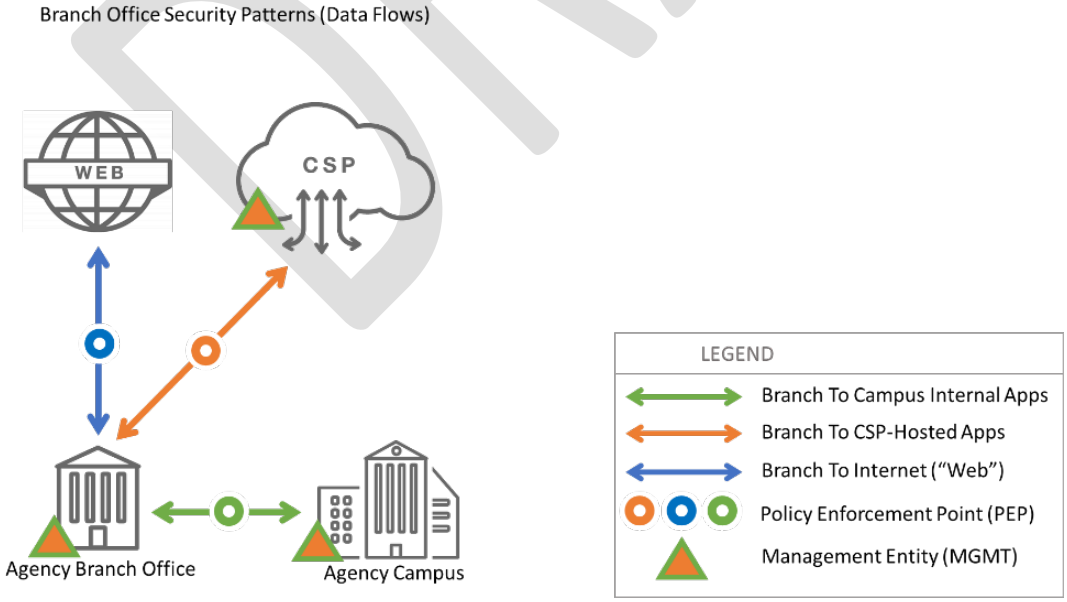
The following are assumptions about the Web:

- 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 Branch Office Use Case is composed of four trust zones: agency campus, agency branch office, CSP, and Web. Branch office network traffic flows to and from an agency campus, to and from an agency CSP, and to and from the Web. A branch office user is able to interact with CSP resources without having to connect directly through the agency. Table 1 describes the components in this security pattern.

Figure 2: Branch Office Security Patterns



[2] "FedRamp," General Services Administration (2019). https://www.fedramp.gov/federal-agencies/.

Table 1: Components in the Branch Office 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, SOC, and other entities. The agency is responsible for defining policies, implementing them in the various PEPs controlled by the agency, and identifying and responding to incidents. Also includes a policy enforcement point between the agency campus and the branch office. This point could include various controls associated with establishing a trusted connection to the branch office, as well as other services to secure the traffic to and from the Web.
Agency Branch Office	The agency branch office trust zone includes a MGMT entity with local scope and facilitates the MGMT functions for the connected PEP. This is managed by the agency. Policy enforcement point between the branch office and other destinations. This point could include various controls associated with establishing a trusted connection to the agency campus, as the interface to agency sanctioned CSP, and as the interface to the Web.
Cloud Service Provider	The CSP providing IaaS/PaaS/SaaS or similar service trust zone. MGMT entity would include locally scoped MGMT functions for connected PEP. The CSP is responsible for protecting the underlying cloud infrastructure with certain defined functions/capabilities managed by the agency. In addition, policy enforcement point between the CSP and the branch office. This point is a shared responsibility deployment model with hardware and software owned and managed by the CSP but may provide some policy definition capabilities to the agency.
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.

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 Branch Office Use Case are outlined in Table 2.

Table 2: Guidance on Applying Universal Security Capabilities in the Branch Office Use Case

Capability	**Use Case Guidance**
Secure Administration	Branch office system components may not permit the same out-of-band administration as components and systems within the agency campus. Secure channels may need to share conveyance mechanisms with other data flows. Agencies must ensure proper protections are in place to permit remote administration and should consider on-site personnel user privileges for disaster recovery, should remote administration fail.
Strong Authentication	Agencies must ensure branch office functions with the same authentication protections as those utilized within the agency campus. This may include a local-to-the-branch authentication service, which permits operation in absence of a connection to the agency campus.
Time Synchronization	Agencies should consider whether the branch office component time synchronization occurs against agency campus sources or duplicates connections to external authoritative time sources. Branch office autonomy, device stratum tolerances, latency, link reliability, component time zone location, and other factors should be considered.
Vulnerability Assessment	The assessment should explicitly consider the case where communication between the branch office and agency campus has failed to make sure additional vulnerabilities are not introduced.
Resilience	The Branch Office Use Case presents the agency with the option to depend upon centralized services or to duplicate services at the branch location. The agency must consider availability, compliance, cost, and administration requirements as well as risk tolerance when making this determination.
Policy Enforcement Parity	When branch office locations are configured to permit connections to CSP and Web services directly, their boundary data protections must align with those established and enforced at the agency campus to ensure a balanced set of protections. Hence, an attacker cannot bypass or evade in/outbound security mechanisms by directing their traffic to take a forwarding path with reduced security rigor.

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 Branch Office Use Case.

Table 3: General Guidance on PEP Capability Groups in the Branch Office Use Case

PEP Capability Group	**Inclusion Justification and Implementation Guidance**
Files	Branch office users will perform information exchanges utilizing file transfers. The agency can either duplicate services at the branch office location for full file analysis or perform some subset of file hygiene tasks and depend upon centralized services for full-feature protections. Some branch locations may be function-specific with unique file types which should have their file protections aligned/tuned to those roles.
Web	Branch locations may have specialized roles that permit a more granular approach to enforcement of Web protections. Agencies can augment their campus policies to increase visibility and control accordingly.
Networking	Connectivity from the branch location to all other resources must be done utilizing all feasible security mechanisms. Traffic forwarding decisions are foundational to information protections. Agencies should consider the branch office reduced device complexity/capacity when making determinations about policy enforcement at the branch location.
DNS	While it is unlikely an agency will be hosting authoritative name services from a branch location, the agency should ensure outbound name resolution requests are properly protected from attack.
Intrusion Detection	Branch locations may have specialized roles that permit a more fine/granular approach to enforcement of IDS protections. Agencies can augment their campus policies to increase visibility and control accordingly.
Enterprise	VPN services provide bulk data encryption between network devices for given source/destination locations.

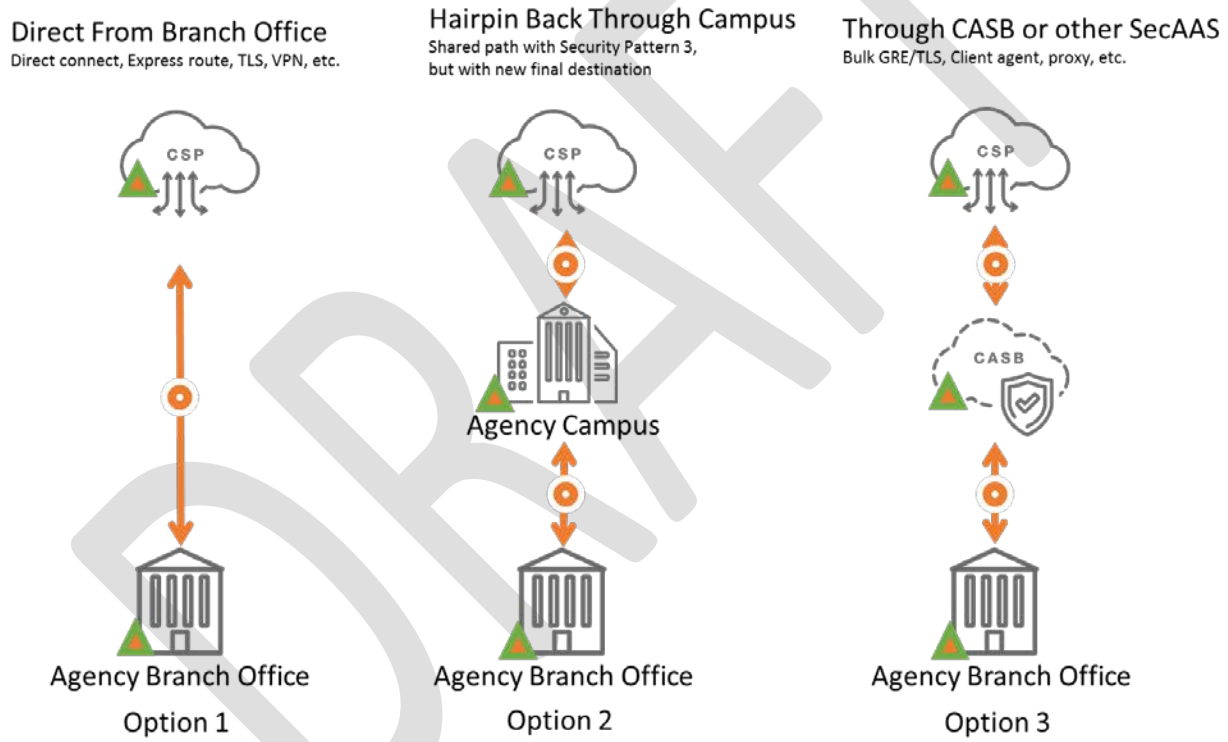
3.5 Security Patterns

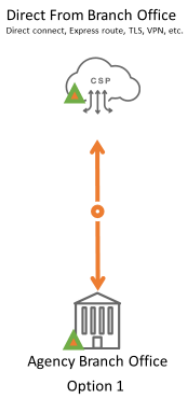
Three security patterns capture the data flows for the agency Branch Office Use Case. Each of these has distinct sources, destinations, and options for policy enforcement. Regardless of the options chosen, due diligence must be practiced ensuring agencies are protecting their information in line with 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 Branch Office Security Pattern 1: Branch Office to Sanctioned CSP Services

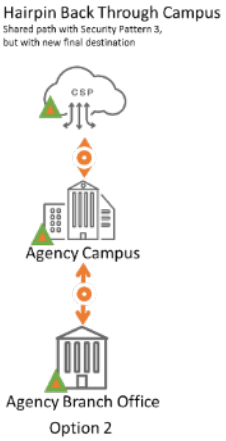
Figure 3 illustrates the first security pattern in the Branch Office Use Case where an agency has deployed services within a CSP environment and then desires to have branch office users or systems interact with the sanctioned CSP services. This data interaction can take place through three options, outlined below.

Figure 3: Security Pattern 1: Branch Office to Sanctioned CSP Services





Option 1 consists of a direct connection from the agency branch office to the sanctioned cloud services. The Branch Office PEP hosts the components which will ensure proper traffic forwarding and eligibility enforcement for sanctioned vs. non-sanctioned destinations for branch office traffic. In addition to basic connectivity, the Branch Office PEP will ensure proper connection and data protections are in place. CSP-hosted protections (PEP and MGMT) will ensure connections for branch office data flows are properly protected and only authorized services and information is being exchanged.



Option 2 consists of a connection from the agency branch office to the sanctioned cloud services, utilizing the agency campus as an intermediary traffic forwarding step. The Branch Office PEP hosts the components which will ensure proper traffic forwarding and protections for all traffic to the agency campus. The Agency Campus PEP ensures protections of connections to the agency branch office and eligibility enforcement for sanctioned vs. non-sanctioned destinations for branch office traffic. CSP-hosted protections (PEP and MGMT) will ensure connections for agency campus data flows are properly protected and only authorized services and information is being exchanged.

Option 3 consists of a connection from the agency branch office to the sanctioned cloud services, utilizing a CASB or other Security-as-a-Service provider as an intermediary forwarding step. The Branch Office 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 sanctioned vs. non-sanctioned destinations for branch office traffic. CSP-hosted protections (PEP and MGMT) will ensure connections for CASB data flows are properly protected and only authorized services and information is being exchanged.

The following PEP Capabilities are applied to Branch Office 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. Supplemental protections that are application-specific may be utilized by the agency. Supplemental implementation guidance specific to this use case is identified for capabilities as applicable in Table 4. Supplemental implementation guidance is not provided for all capabilities.

Table 4: Branch Office Security Pattern 1: TIC PEP Capabilities

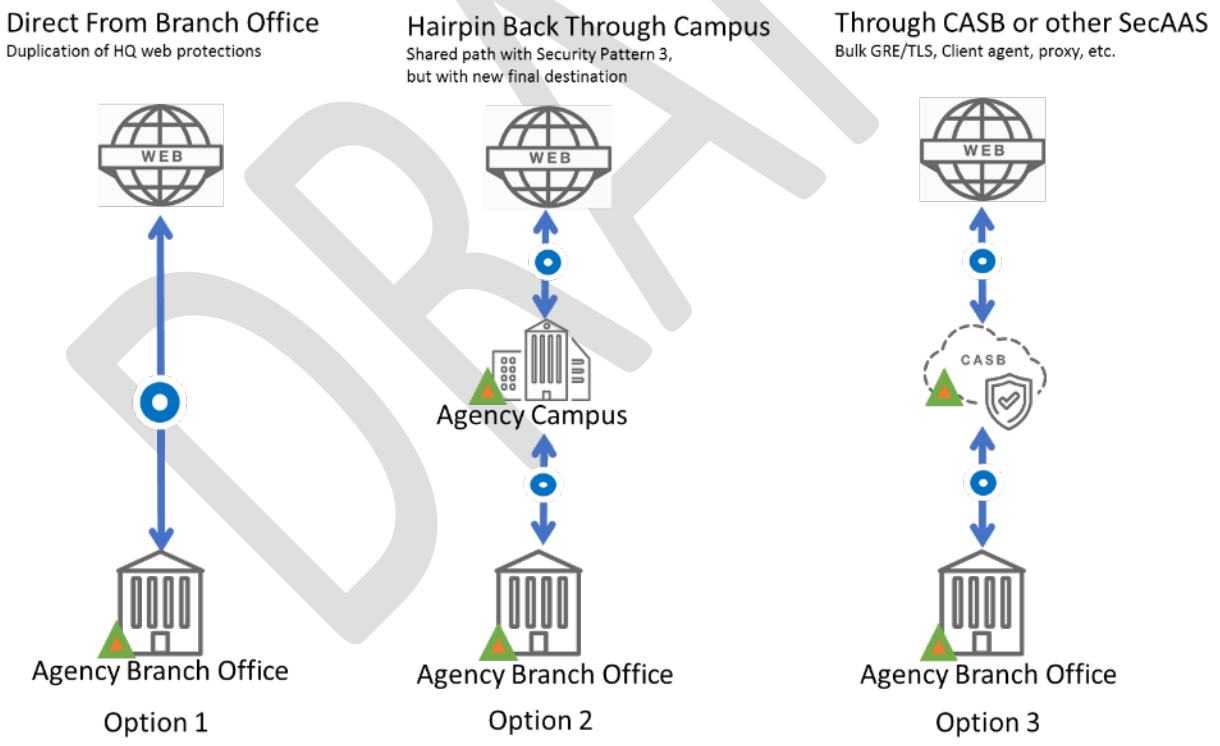
PEP Capability Group	**PEP Capability**	**Implementation Guidance**
Files	Anti-malware	Ensure consistent policies with agency campus.
	Content Disarm & Reconstruction	May be able to be tuned to branch office functions.
Web	Break and Inspect	No supplemental guidance
	Active Content Mitigation	No supplemental guidance
	Certificate Blacklisting	No supplemental guidance
	Certificate Consensus	No supplemental guidance
	Content Filtering	No supplemental guidance
	Authenticated Proxy	No supplemental guidance
	Data Loss Prevention	No supplemental guidance
	DNS-over-HTTPS Filtering	No supplemental guidance
	RFC Compliance Enforcement	No supplemental guidance
	Domain Category Filtering	No supplemental guidance
	Domain Reputation Filter	No supplemental guidance
	Bandwidth Control	Branch office locations may have reduced link capacity, increasing the importance of managed utilization.
	Malicious Content Filtering	No supplemental guidance
	Access Control	No supplemental guidance
Networking	Network Access Controls	Branch office locations may have reduced physical protections, increasing the importance of device-level connectivity vetting.
	IP Blacklisting	This can be used to ensure all non-sanctioned CSP destinations remain unreachable.
DNS	DNS Blackholing	No supplemental guidance
	DNSSEC for agency Clients	The branch office should leverage the same name resolution protections as the agency campus.

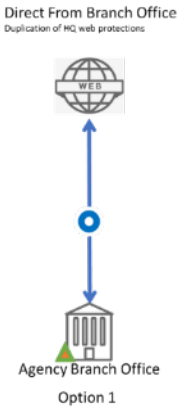
Intrusion Detection	Endpoint Detection and Response	No supplemental guidance
	Intrusion Protection Systems (IPS)	No supplemental guidance
	Adaptive Access Control	The branch office may have unique operating hours or other restrictions permitting a more rigorous access control policy.
Enterprise	Shadow IT Detection	Sanctioned CSP services must be differentiated and permitted in a manner such that unsanctioned services from the same CSP are prohibited.

3.5.2 Branch Office Security Pattern 2: Branch Office to Web

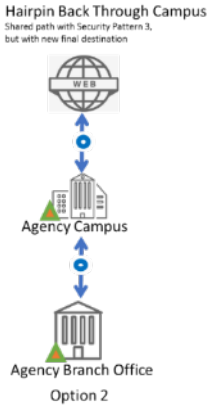
Figure 4 illustrates connections from the branch office which are destined for Web-based systems. There are three options for this connectivity. Connections in this security pattern are the riskiest, as there is a connection from the agency branch office to the untrusted Web. This will require the greatest amount of rigor to be applied to capabilities in place in the Branch Office PEP.

Figure 4: Security Pattern 2: Branch Office to Web

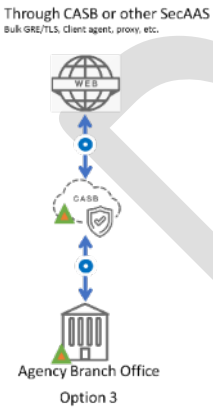




Option 1 depicts a direct connection from the agency branch office to the Web for user web connections. The Branch Office PEP ensures traffic is forwarded to the Web and all applicable security policies are enforced. Care must be taken by the agency to ensure the same protections are applied to all traffic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



Option 2 depicts a connection from the agency branch office to the Web for user web connections, utilizing the agency campus as an intermediary traffic forwarding step. The Branch Office PEP ensures traffic is forwarded to the agency with appropriate connection security. The Agency Campus PEP ensures both connection security to the branch office and all applicable security policies are enforced for connections destined for the Web. Since traffic from the branch office and agency campus takes the same forwarding path, the same protections are applied to all traffic destined for the Web, regardless of origin.



Option 3 depicts a connection from the agency branch office to the Web for user web connections, utilizing a CASB or other Security-as-a-Service provider as an intermediary traffic forwarding step. The Branch Office PEP ensures traffic is forwarded to the CASB with appropriate connection security. The CASB PEP ensures both connection security to the branch office 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 following PEP Capabilities are applied to Branch Office 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. Supplemental implementation guidance specific to this use case is identified for capabilities as applicable in Table 5. Supplemental implementation guidance is not provided for all capabilities.

Table 5: Branch Office Security Pattern 2: PEP Capabilities

PEP Capability Group	PEP Capability	Implementation Guidance
Files	Anti-malware	Ensure consistent policies with agency campus.
	Content Disarm & Reconstruction	May be able to be tuned to branch office functions.
Web	Break and Inspect	No supplemental guidance
	Active Content Mitigation	No supplemental guidance
	Certificate Blacklisting	No supplemental guidance
	Certificate Consensus	No supplemental guidance
	Content Filtering	No supplemental guidance
	Authenticated Proxy	No supplemental guidance
	Data Loss Prevention	No supplemental guidance
	DNS-over-HTTPS Filtering	No supplemental guidance
	RFC Compliance Enforcement	No supplemental guidance
	Domain Category Filtering	No supplemental guidance
	Domain Reputation Filter	No supplemental guidance
	Bandwidth Control	Branch office locations may have reduced link capacity, increasing the importance of managed utilization.
	Malicious Content Filtering	No supplemental guidance
	Access Control	No supplemental guidance
Networking	Network Access Controls	Branch office locations may have reduced physical protections, increasing the importance of device-level connectivity vetting.
	IP Blacklisting	No supplemental guidance
	Network Segmentation	Ensure only required subnets are able to reach Web proxy components and receive subsequent replies.

DNS	DNS Blackholing	No supplemental guidance
	DNSSEC for agency Clients	The branch office should leverage the same name resolution protections as the agency campus.
Intrusion Detection	Endpoint Detection and Response	No supplemental guidance
	Intrusion Protection Systems (IPS)	No supplemental guidance
	Adaptive Access Control	The branch office may have unique operating hours or other restrictions permitting a more rigorous access control policy.
Enterprise	Shadow IT Detection	No supplemental guidance

3.5.3 Branch Office Security Pattern 3: Branch Office to Agency Internal Services

As shown in Figure 5, entities within the branch office can access resources within the agency campus. This security pattern is relevant to TIC only when Branch Office Security Pattern 1 and/or Branch Office Security Pattern 2 are in use. Connection security robustness is enforced by both PEPs to ensure consistent application of relevant security capabilities is applied. Since an agency has control of both the agency campus and branch office, the agency can determine the level of rigor for security capabilities applied to traffic between the two. Due diligence must be practiced ensuring agencies are protecting their information in line with their risk tolerances. Conveyance between the agency campus and the branch office may be via point-to-point, SD-WAN, leased line, VPN, etc.

Figure 5: Security Pattern 3: Branch Office to Agency Internal Services

The following PEP Capabilities are applied to Branch Office Security Pattern 3. 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 6: Branch Office Security Pattern 3: TIC PEP Capabilities

PEP Capability Group	PEP Capability	Implementation Guidance
Networking	Network Access Controls	Branch office locations may have reduced physical protections, increasing the importance of device-level connectivity vetting.
	IP Blacklisting	This can be used to ensure all non-sanctioned CSP destinations remain unreachable.
Enterprise	VPN	All traffic from the branch office shares a destination of the agency campus, permitting bulk encryption and consistent traffic forwarding policies to be applied.

3.6 Telemetry Requirements - Information Sharing with CISA

As agencies transition to direct connections from agency branch offices to external services, visibility by CISA must be preserved through information sharing. Figure 6 shows the conceptual architecture of the Branch Office 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 6: Branch Office Telemetry Sharing with CISA

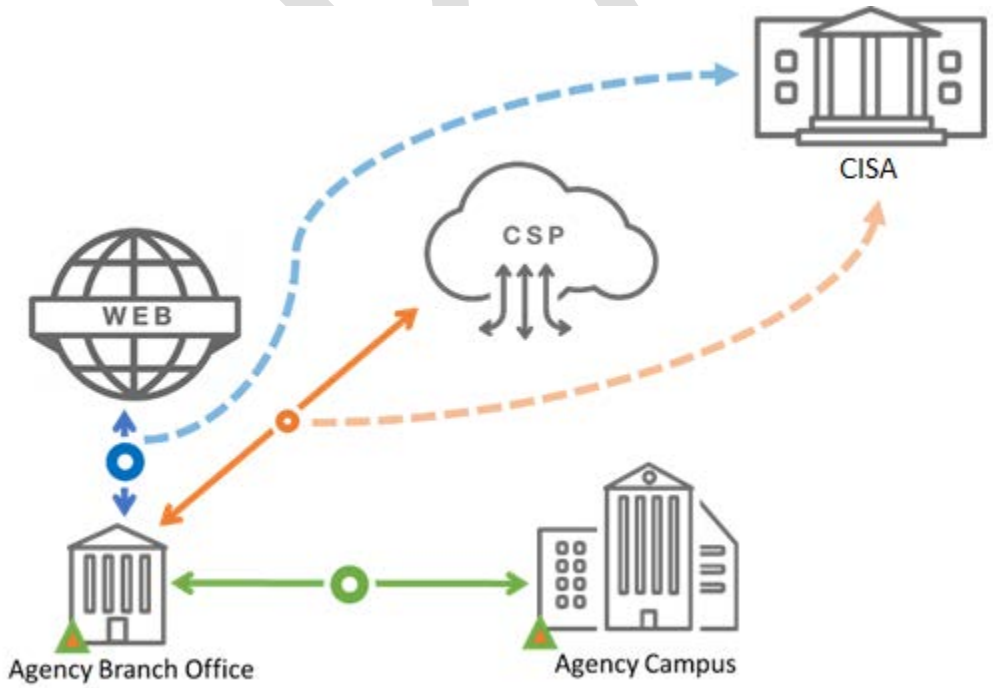
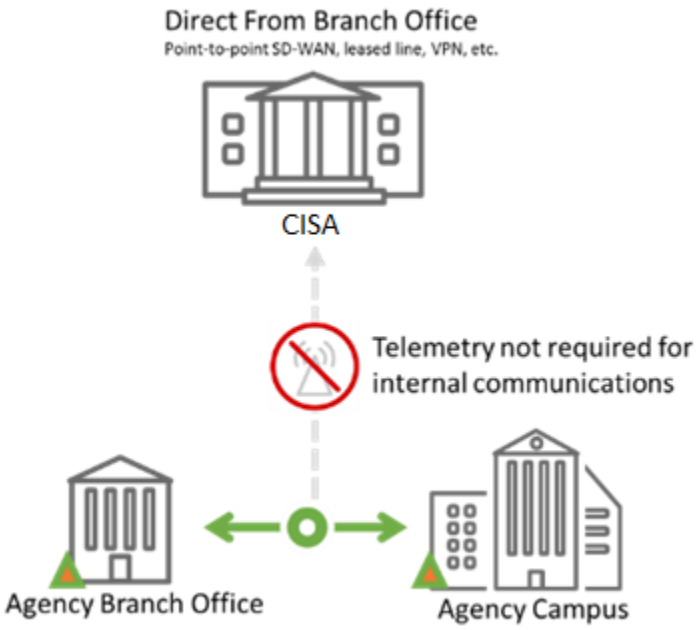


Figure 7 clarifies that there are no requirements to send telemetry data to CISA for agency internal data flows. The requirements for sharing telemetry data with CISA are only required on the data flows between the branch office and the Web, as well as on the data flows between the branch office and any CSPs.

Figure 7: Information sharing with CISA Exception for Internal Communications



4. Conclusion

This document provides guidance on how an agency can configure its branch office 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 any TIC Overlays that are applicable to service providers that an agency employs.

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.