TLP:CLEAR

Trusted Internet Connections 3.0

Branch Office Use Case

April 2023
Version 2.0
Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

REVISION HISTORY

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

Table 1: Revision History Table

Version	Date	Revision Description	Section/Page Affected
Draft	December 2019	Initial Release	All
1.0	April 2021	Response to RFC and Stakeholder Feedback	All
2.0	April 2023	Added 6 Universal Security Capabilities: User Training and Awareness; Supply Chain Risk Management; Resource Lifecycle Management; Security Test and Exercise; Continuous Monitoring Reporting; Governance and Policy Auditing	Pg. 19, 20
		Updated Web PEP Security Capability definition for Domain Name Resolution Filtering	Pg. 23
		Added 2 DNS PEP Security Capabilities: Domain Name Monitoring; CISA's Protective DNS Service; removed EINSTEIN 3 Accelerated Domain Name Protections from DNS PEP	Pg. 27
		Added 1 Intrusion Detection PEP Security Capability: Network Detection and Response Security Capability	Pg. 29
		Added 2 Data Protection PEP Security Capabilities:	Pg. 31

Version	Date	Revision Description	Section/Page Affected
		Data Labeling; Data Inventory	
		Added 7 Identity PEP Security Capabilities: Adaptive Authentication; Entitlement Inventory; Secrets Management; Behavioral Baselining; Enterprise Identity and Access Management; Multi-factor Authentication; and Continuous Authentication	Pg. 32, 33
		Updated References	Throughout document
		Added Appendix B	Pg. 37

This use case references *Trusted Internet Connections 3.0 Security Capabilities Catalog,* v3.0, dated April 2023. The applicable security capabilities will be further explained in the document.

READER'S GUIDE

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

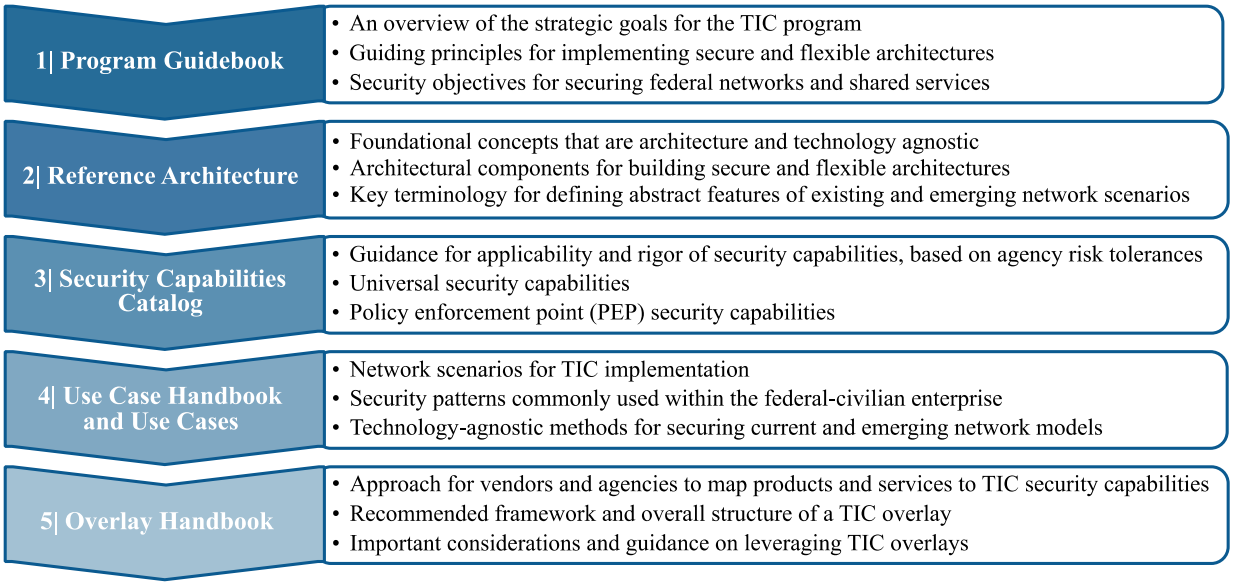

Figure 1: TIC 3.0 Guidance Snapshot

CONTENTS

Figures

Tables

1. INTRODUCTION

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

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

1.1 KEY TERMS

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

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

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

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

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

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

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

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

---

[1] "Update to the Trusted Internet Connections (TIC) Initiative," Office of Management and Budget M-19-26 (2019). https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf.
[2] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R5)," September 2020. http://dx.doi.org/10.6028/NIST.SP.800-53r5.

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

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

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

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

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

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

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

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

2. OVERVIEW OF THE TIC USE CASES

TIC use cases provide guidance on the secure implementation and configuration of specific platforms, services, and environments, and will be released on an individual basis. The guidance is derived from pilot programs and best practices from the public and private sectors. The purpose of each TIC use case is to identify the applicable security architectures, data flows, and policy enforcement points (PEPs) and to describe the implementation of the security capabilities in a given scenario. TIC use cases articulate:

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

TIC use cases build upon the key concepts and conceptual implementation of TIC 3.0 presented in the *TIC 3.0 Reference Architecture* (Reference Architecture) and provides implementation guidance for applicable security capabilities defined in the *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog). The *TIC 3.0 Use Case Handbook* (Use Case Handbook) provides general guidance for how agencies can use and combine use cases.

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

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

- Each trust zone in a use case will be labeled with a high, medium, or low trust level, based on a pilot implementation or best practice. The use cases are depicted following the schema illustrated in Figure 2. Agencies can modify this trust zone designation to meet their needs. Refer to the Reference Architecture for more details on trust zones.

Figure 2: Use Case Trust Zone Legend

- When securing trust zones, agencies should consider unique data sensitivity criteria and the impact of compromise to agency data stored in trust zones. Agencies may apply additional security capabilities that have not been included in the use case.
- Agencies have the discretion to determine the level of rigor necessary for applying security capabilities in use cases, based on federal guidelines and their risk tolerance.

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

3. PURPOSE OF THE BRANCH OFFICE USE CASE

The *TIC 3.0 Branch Office Use Case* (Branch Office Use Case) defines how network and multi-boundary security should be applied when an agency conducts work in more than one physical location, in which most of the information technology (IT) services, including generic web traffic, are traditionally provided by the agency campus. This use case helps agencies gain application performance (e.g., latency, throughput, jitter, etc.); reduce costs (e.g., 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* (Traditional TIC Use Case) enumerates the protections for agency campus and will not be repeated here.

This use case includes three network security patterns:

- Secure branch office access to agency-sanctioned cloud service providers (CSPs),
- Secure branch office access to web, and
- Secure branch office access to agency campus.

An agency may implement a subset of these security patterns rather than all three. For instance, an agency may not yet have agency-sanctioned cloud services with authorized direct connectivity from a branch office location. In cases like these, the agency may only implement the branch office to web and branch office to agency campus security patterns.

Agencies may implement additional security patterns, though they may be out of scope for the Branch Office Use Case.

Agencies may implement additional security patterns. These additional security patterns may be in scope for a different use case but would be out of the scope of the Branch Office Use Case.

4. ASSUMPTIONS AND CONSTRAINTS

This section outlines guiding assumptions and constraints for the Branch Office Use Case. It is intended to clarify significant details about the construction and replication of this use case. The assumptions are broken down by the use case as a whole and by the unique entities discussed in the use case:

- Agency campus,
- Branch office,
- Agency-sanctioned CSPs, and
- Web.

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

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

The following are assumptions about the agency campus.

- The agency campus uses the Traditional TIC Use Case, or equivalent, to access the web and CSPs.
- The agency maintains control over and has significant visibility into the agency campus.
- Data is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- The agency employs network operation center (NOC) and security operation center (SOC) tools capable of maintaining and protecting their 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.

- Traditionally, the branch office would have used the agency campus for external web and CSP traffic.
- The agency maintains control over and has significant visibility into the branch office.
- Data is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- The agency employs NOC and SOC tools capable of maintaining and protecting the branch office infrastructure. These functions may be performed as an extension to the NOC and SOC tools managed and housed at the agency campus, as separate functions local to the branch office, or via commensurate solutions.

[3] "National Cybersecurity Protection System (NCPS)," Cybersecurity and Infrastructure Security Agency. https://cisa.gov/national-cybersecurity-protection-system-ncps.
[4] "Continuous Diagnostics and Mitigation (CDM)," Cybersecurity and Infrastructure Security Agency. https://cisa.gov/cdm.

The following are assumptions about agency-sanctioned CSPs.

- CSPs are compliant with the Federal Risk and Authorization Management Program (FedRAMP)[5].
- Interactions with CSPs 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 CSPs.
- The agency has limited control over and visibility into CSP environments.
- CSPs have NOCs and SOCs that control and protect the portions of the service infrastructure where the agency has little or no control or visibility.
- The agency only uses secure mechanisms (e.g., transport layer security (TLS) or VPN) to communicate with CSPs.
- The agency only uses strong authentication mechanisms (e.g., Federal Information Processing Standard (FIPS) 140-2[6] complaint multi-factor authentications (MFA)) with CSPs.
- Data stored at CSPs is protected at a level commensurate with the agency's risk tolerance and in accordance with federal guidelines.
- CSPs allow the agency to define or configure policies that the CSP applies on their behalf and allows the agency to define roles and responsibilities for the configuration of those policies.
- CSPs provide the agency with mechanisms for obtaining visibility into the current state and history of the system (e.g., log information).
- CSPs provide commensurate 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 entities.
- The agency cannot apply policy in the web.

[5] "FedRAMP," General Services Administration (2019). https://www.fedramp.gov/federal-agencies/.
[6] "Federal Information Processing Standard 140-2," National Institute of Standards and Technology (2019). https://csrc.nist.gov/publications/detail/fips/140/2/final.

5. CONCEPTUAL ARCHITECTURE

The Branch Office Use Case focuses on the scenario in which branch office network traffic flows to and from an agency campus, to and from agency CSPs, and to and from the web. In this scenario, a branch office user can interact with CSP resources without having to connect directly through the agency campus. As shown in Figure 3, this use case is composed of four trust zones: agency campus, agency branch office, CSP, and web.

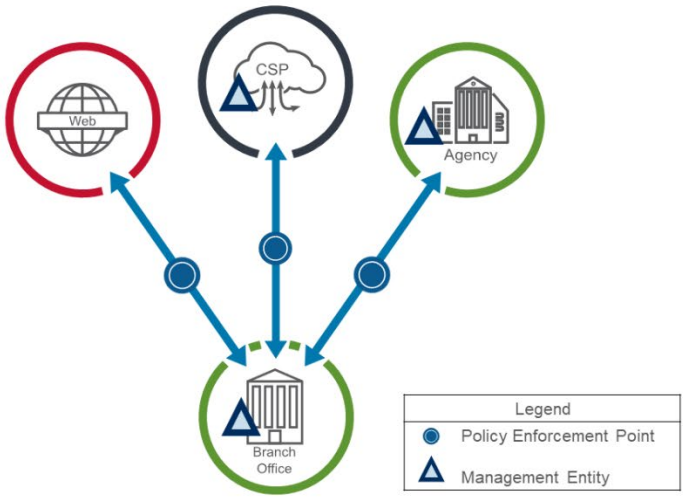

Figure 3: Branch Office Conceptual Architecture

These trust zones are detailed in Table 2. To simplify the visualization and descriptions, the use case shows a single CSP trust zone. However, this simplification is not meant to imply that an agency must treat all CSPs in the same manner. Applicable TIC capabilities and their rigor should be tailored for the nature of the CSP service in use.

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

Implementation Consideration

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

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

Table 2: Trust Zones in the Branch Office Use Case

Trust Zone	Description
Agency Campus Trust Zone	The Agency Campus Trust Zone is the logical zone for the agency campus or the agency's enterprise network. The trust zone includes management entities (MGMTs) such as the NOC, SOC, and other entities. The agency maintains control over and visibility into the agency campus. It is responsible for defining policies, implementing them in the various PEPs controlled by the agency, and identifying and responding to incidents. Policy enforcement between the agency campus and the branch office 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 agency services. The agency campus accesses external entities through the Traditional TIC Use Case, or equivalent, when accessing external entities or when transiting traffic from the branch office to external entities. The Agency Campus Trust Zone is labeled with a ***high trust level*** in this use case.
Branch Office Trust Zone	The Branch Office Trust Zone is a logical trust zone for an agency branch office. The agency maintains control over and visibility into the agency branch office. This trust zone may include a MGMT with local scope, facilitating management functions for the connected PEPs. The PEPs between the branch office and other destinations allow for the policy definition to be set by the agency. These points could include controls associated with establishing a trusted connection to the agency campus and interfacing to agency-sanctioned CSPs and the web. The Branch Office Trust Zone is labeled with a ***high trust level*** in this use case.
Cloud Service Provider Trust Zone	The CSP Trust Zone is a logical trust zone for the CSP providing Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, or a similar service. The agency has limited control over and visibility into the CSP environment, with the CSP responsible for protecting the underlying cloud infrastructure and the agency providing certain defined functions and capabilities to manage. The trust zone includes a MGMT that executes locally scoped functions for the CSP environment. The PEP between the CSP and the branch office may be a shared responsibility deployment model with hardware and software owned and managed by the CSP and some policy definition capabilities available to the agency. The CSP Trust Zone is labeled with a ***medium trust level*** in this use case.
Web Trust Zone	The Web Trust Zone is a logical trust zone that depicts an environment with untrusted external services, including non-agency-sanctioned cloud service providers, where neither the agency nor entities acting on its behalf, may deploy or enforce policies. Given these limitations, the Web Trust Zone is labeled with a ***low trust level*** in this use case.

6. SECURITY PATTERNS

Three security patterns capture the data flows for the Branch Office Use Case. Each has distinct sources, destinations, and options for policy enforcement. Regardless of the options chosen, due diligence must be practiced, ensuring agencies are protecting their information in line with their risk tolerances, especially in instances where security policies are being applied by a third party on an agency's behalf. When additional security capabilities are necessary to manage residual risk, agencies should apply the controls or explore options for compensating capabilities that achieve the same protections to manage risks.

The security patterns include the following trust zone destinations:

- CSP,
- Web, and
- Agency campus.

6.1 SECURITY PATTERN 1: BRANCH OFFICE TO CLOUD SERVICE PROVIDER

Figure 4 illustrates the first security pattern in the Branch Office Use Case where an agency has deployed services within a CSP environment and desires to have branch office users or systems interact with the agency-sanctioned CSP services. This data interaction can take place through three options, outlined below.

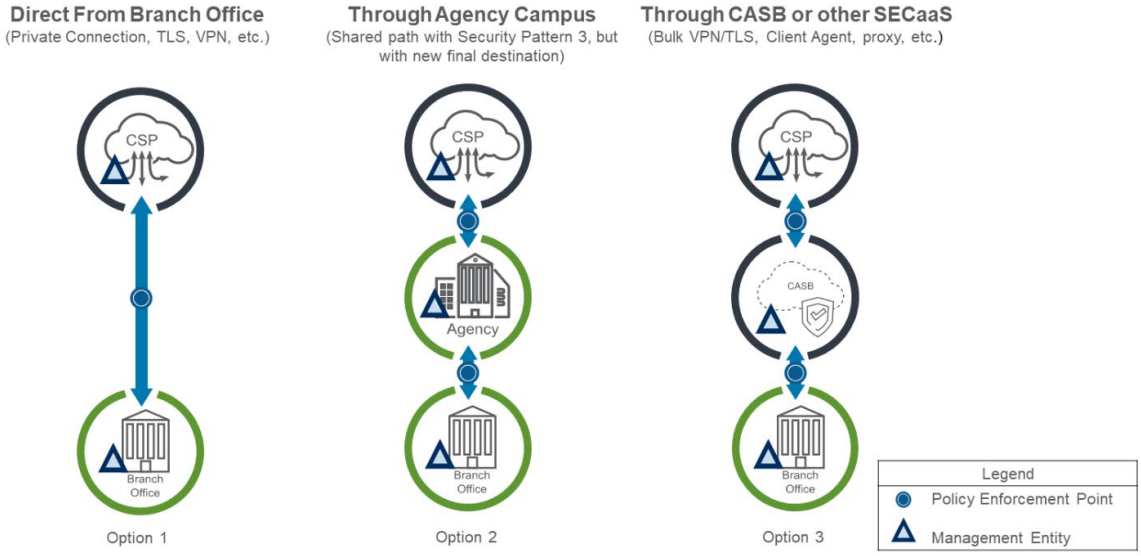

Figure 4: Security Pattern 1: Branch Office to Cloud Service Provider

Implementation Consideration

Agencies may employ capabilities at the branch office, CASB or CSP so long as commensurate protections are maintained between the branch office and the CSP.

The **first option** (left) permits direct access to sanctioned cloud resources directly from the branch office. Entities within the branch office either establish a protected connection to the CSP or use an existing protected connection established with the CSP to connect to CSP resources. These protected connections may go through a private connection between the agency and the CSP, or through shared infrastructure (e.g., the internet). Policy enforcement placement and protections may be applied at the branch office and the sanctioned CSP. Capabilities traditionally handled by agency campus services, or commensurate capabilities, may be deployed at the branch office or the sanctioned CSP so long as policy enforcement parity is ensured.

The **second option** (left) aligns with traditional mechanisms for accessing sanctioned cloud resources and may use data flows also defined in the Traditional TIC Use Case. Entities within the branch office either establish a protected connection to the agency campus or use an existing protected connection established with the agency campus to connect to CSP resources. Policy enforcement can be performed at the branch office, agency campus, and CSP. This option facilitates common connectivity to CSP resources for both campus and branch office users. This may include dedicated connections to the CSP with enhanced performance, security, or other enhancements. Eligibility enforcement for CSP access can rely upon connection origin as an additional attribute for policies.

The **third option** (left) permits connectivity from entities within the branch office to agency-sanctioned CSP resources through a CASB or other Security-as-a-Service (SECaaS) provider. Policy enforcement can be performed at the branch office, CASB, and CSP. Policy enforcement parity between agency campus and branch office users can be simplified when both use the same CASB or SECaaS provider. Entities within the branch office either establish a protected connection to the CASB or use an existing protected connection established with the CASB. Various methods can be used to direct entity traffic to the CASB, including client agents, proxy settings, and domain name system (DNS) means. Given the more limited control and visibility available to the agency, the CASB Trust Zone is labeled with a ***medium trust level*** in this option.

6.2 SECURITY PATTERN 2: BRANCH OFFICE TO WEB

Figure 5 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 because of the connection to an untrusted entity. This will require the greatest amount of rigor to be applied to security capabilities in the PEP at the branch office.

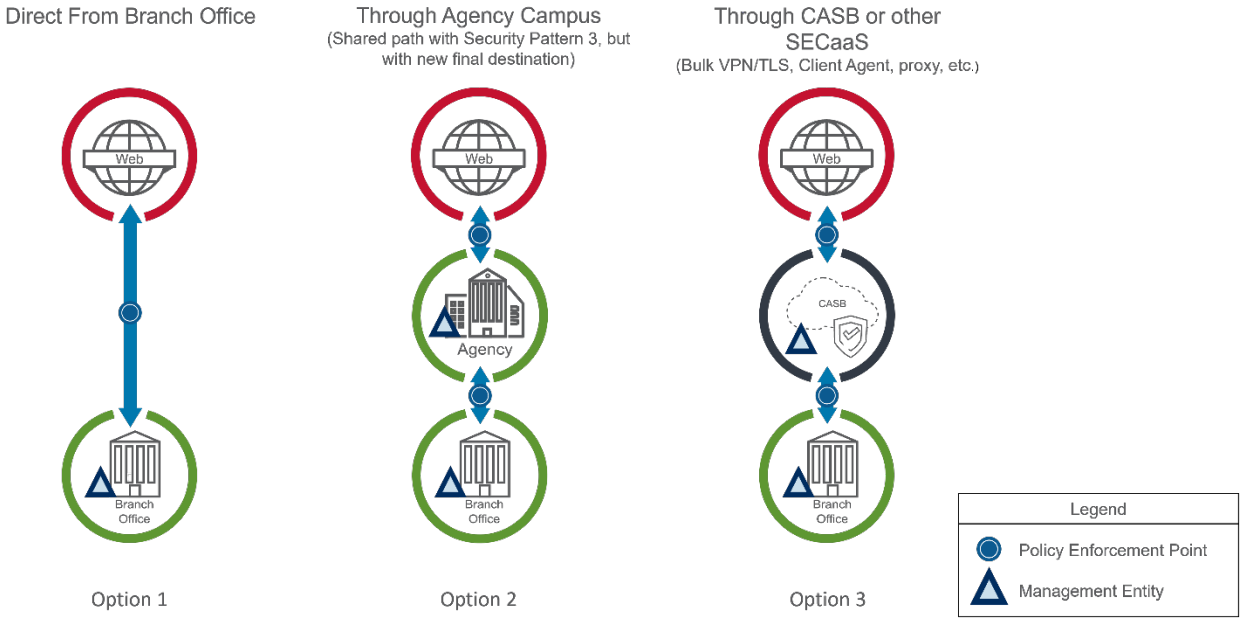

Figure 5: Security Pattern 2: Branch Office to Web

Implementation Consideration

Agencies should apply the greatest rigor to security capabilities for the connections between the branch office and the web.

In the **first option** (left), entities within the branch office can access the web directly. Policy enforcement placement and protections are applied at the branch office. Security capabilities traditionally handled by agency campus services may be deployed to the branch office so long as policy enforcement parity is ensured.

The **second option** (left) aligns with traditional mechanisms for accessing the web and may utilize data flows also defined in the Traditional TIC Use Case. Entities within the branch office either establish a protected connection to the agency campus or use an existing protected connection established with the agency campus to connect to the web. Policy enforcement can be performed at the branch office and agency campus. This option facilitates common connectivity to the web for both agency campus and branch office users.

The **third option** (left) permits connectivity from entities within the branch office to the web through a CASB or other SECaaS provider. Policy enforcement can be performed at the branch office and CASB. Policy enforcement parity between agency campus and branch office users can be simplified when both use the same CASB or SECaaS provider. Entities within the branch office either establish a protected connection to the CASB or use an existing protected connection established with the CASB. Various methods can be used to direct entity traffic to the CASB, including client agents, proxy settings, and DNS means. Given the limited control and visibility available to the agency, the CASB Trust Zone is labeled with a ***medium trust level*** in this option.

6.3 SECURITY PATTERN 3: BRANCH OFFICE TO AGENCY CAMPUS

Figure 6 illustrates connections from the branch office to services hosted at the agency campus. This security pattern may be relevant to other security patterns that route traffic through the agency. There are two options for this connectivity. Since the agency controls both the agency campus and branch office, the agency can determine the level of rigor for security capabilities to apply to traffic between the two. Due diligence must be practiced to ensure the agency is protecting their information in line with their risk tolerances.

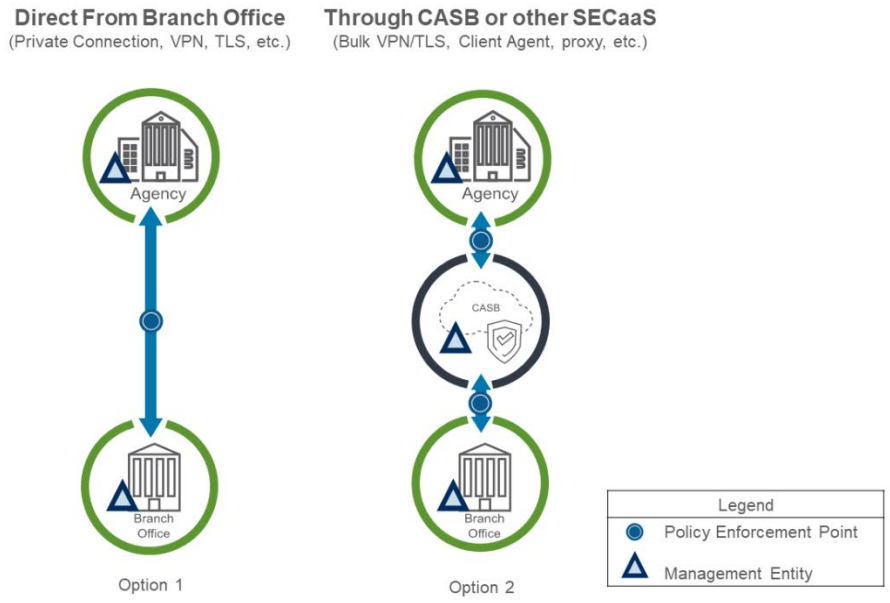

Figure 6: Security Pattern 3: Branch Office to Agency Campus

Implementation Consideration

Since the agency controls both the agency campus and branch office, agencies may determine the location and level of rigor to apply to security capabilities.

In the **first option** (left), entities within the branch office either establish a protected connection to the agency campus or use an existing protected connection established with the agency campus to connect to agency services. These protected connections may go through a private connection between the branch office and the agency campus, or through shared infrastructure (e.g., the internet). Policy enforcement placement and protections may be applied at the branch office and the agency campus. This option aligns with traditional mechanisms for accessing the agency campus and may utilize data flows also defined in the Traditional TIC Use Case.

The **second option** (left) permits connectivity from entities within the branch office to the agency campus through a CASB or other SECaaS provider. Policy enforcement can be performed at the branch office, the CASB, and the agency campus. Policy enforcement parity between the agency campus and multiple branch office locations can be simplified when the locations use the same CASB or SECaaS provider. Entities within the branch office either establish a protected connection to the CASB or use an existing protected connection established with the CASB. Various methods can be used to direct entity traffic to the CASB, including client agents, proxy settings, and DNS means. Given the more limited control and visibility available to the agency, the CASB Trust Zone is labeled with a ***medium trust level*** in this option.

7. APPLICABLE SECURITY CAPABILITIES

The Security Capabilities Catalog contains a table of universal and PEP security capabilities that apply across use cases, but not all are applicable to every use case. Each use case will contain a set of relevant security capabilities, based on agency pilot implementations and best practices. Additional security capabilities may be employed by agencies to reflect agency requirements, risk tolerances, and other factors. For traceability, the security capabilities not included in this use case are listed below by PEP capability group.

- Email: All capabilities in this functional group are not applicable.
- Networking: Resource Containment
- Resiliency: Elastic Expansion
- DNS: Domain Name Validation for Agency Domains
- Intrusion Detection: Deception Platforms and Certificate Transparency Log Monitoring
- Enterprise: Application Container, Remote Desktop Access, and Costs Monitoring
- Unified Communications and Collaboration (UCC): All capabilities in this functional group are not applicable.
- Services: All capabilities in this functional group are not applicable.
- Identity: Service Identity

7.1 UNIVERSAL SECURITY CAPABILITIES

Universal security capabilities are enterprise-level capabilities that outline guiding principles for TIC use cases and apply across use cases. Agencies have the discretion to determine the level of rigor necessary for applying universal security capabilities based on federal guidelines and their risk tolerance.

Table 3 provides a list of the universal security capabilities that apply to the Branch Office Use Case, and implementation guidance for agencies to consider. Most agencies will have an existing enterprise solution for the universal security capabilities; so, as agencies deploy the Branch Office Use Case, the guidance below can be integrated into their existing solutions. While universal security capabilities are broadly applicable, the circumstances and threats associated with a branch office require agencies to consider the security challenges that may need to be addressed.

Table 3: Universal Security Capabilities

Capability	Description	Use Case Guidance
Backup and Recovery	Backup and recovery entails keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures, or corruption.	Branch office configuration and data should be backed up, if possible, to a separate location (e.g., agency, externally-hosted backup service). Agencies should consider when the connection between the agency and the branch office is disrupted.
Central Log Management with Analysis	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	The agency's log management solution should integrate telemetry from the branch office. If branch offices can directly interact with CSPs, the agency should integrate telemetry from the CSP into their analysis for visibility into the branch office's utilization of CSP services, even if telemetry cannot be obtained from the branch office (e.g., if the connection between the agency and the branch office is disrupted).
Configuration Management	Configuration management is the implementation of a formal plan for documenting, and managing, changes to the environment, and monitoring for deviations, preferably automated.	Agency configuration management should be followed for services and entities in the branch office. These procedures may be applied centrally by the agency but should consider when the connection between the agency and the branch office is disrupted.
Incident Response Planning and Incident Handling	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.	Agency incident response and handling should consider the branch office. Incident response may be handled centrally by the agency or by an entity acting on its behalf. Incident response plans should consider when the connection to the branch office is disrupted. This may include updating roles and responsibilities to account for response personnel located at a branch office. When implementing responses to security incidents, responders should account for alternative access available to the CSPs by branch office users.

Capability	Description	Use Case Guidance
Inventory	Inventory entails developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and restricted from gaining access.	Agency inventories should integrate branch office information as well as information about the cloud services being used by the branch office.
Least Privilege	Least privilege is a design principle whereby each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	Agencies should, if possible, limit the methods of direct access to agency-sanctioned CSPs to those branch office users and entities that require access to the CSP service. Agencies should consider the privileges of the system administration support personnel at the branch office and ensure it aligns with the roles and functions of those individuals. Privileges for branch office users should ensure commensurate protections are in place to align with agency campus data protections.
Secure Administration	Secure administration entails performing administrative tasks in a secure manner, using secure protocols.	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	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	Agencies should ensure branch office functions with equivalent or better authentication protections[7] as those used within the agency campus. These authentication procedures may be handled centrally by the agency

[7] CISA Phishing-Resistant Multifactor Authentication, www.cisa.gov/mfa.

Capability	Description	Use Case Guidance
		but should account for situations where the connection with the branch office is disrupted.
Time Synchronization	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clocks and enable accurate comparison of timestamps between systems.	Branch office endpoints should be synchronized. Agencies should consider whether the branch office component time synchronization occurs against agency campus sources or uses external authoritative time sources. Branch office autonomy, device stratum tolerances, latency, link reliability, component time zone location, and other factors should be considered.
Vulnerability Management	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	Agencies should integrate the branch office into their overall vulnerability assessment procedures. These procedures should include assessments of the branch office, assessments of the CSP environment that account for the new access points, and assessments of the connections between the agency campus and the branch office. The assessments should explicitly consider the case where communication with the branch office is disrupted to ensure additional vulnerabilities are not introduced.
Patch Management	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	Agencies should integrate the branch office into their overall patch management solution. These patch management solutions may be handled centrally but should account for how the loss of connectivity to the agency campus or authorized CSPs might affect patch deployment to entities in the branch office.

Capability	Description	Use Case Guidance
Auditing and Accounting	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	Cloud service licensing, activity, and billing may require adaptation to existing tracking mechanisms. Agencies should ensure compatibility and interoperability to minimize visibility gaps.
Resilience	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	Agencies should determine which services can be centralized and which can be deployed at the branch location. The agency should consider availability, compliance, cost, and administration requirements as well as risk tolerance when making this determination. Connection resilience between the agency campus and branch office locations may be enhanced by leveraging multiple means of conveyance (e.g., redundant links, software-defined wide area networking (SD-WAN) techniques, etc.). In these situations, path priorities, security function order of execution, and policy enforcement should ensure security parity on all conveyance paths.
Enterprise Threat Intelligence	Enterprise threat intelligence is the usage of threat intelligence from private or government sources to implement mitigations for the identified risks.	Agencies should seek out and adopt any new threat intelligence feeds which align with threats to the users and services at the branch office.
Situational Awareness	Situational awareness is maintaining effective current and historical awareness across all components.	Agencies should maintain awareness of the branch office locations, and their users, including threats that may be specific to those users or locations. Agencies should seek to integrate CSP telemetry and branch office telemetry into agency situational awareness tools.

Capability	Description	Use Case Guidance
Dynamic Threat Discovery	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	Agencies should track the branch office use of agency services or data to look for changes or discrepancies, including the use of agency services by branch office employees outside the branch office location, or non-branch office employees using agency services from the branch office location.
Policy Enforcement Parity	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding paths, or endpoints used.	When branch office locations allow for direct connections to CSP and web services, their boundary data protections should align with those established and enforced at the agency campus to ensure a balanced set of protections. Hence, an attacker cannot bypass or evade security mechanisms by directing their traffic to take a forwarding path with reduced security rigor. If multiple means of conveyance are employed (e.g., redundant links, SD-WAN, etc.), path priorities, security function order of execution, and policy enforcement should ensure security parity on all conveyance paths.
Effective Use of Shared Services	Effective use of shared services means that shared services are employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	Agencies should consider security capabilities when selecting shared service providers. Agencies should consider regional delivery opportunities so that shared services can be deployed closer to branch office locations.
Integrated Desktop, Mobile, and Remote Policies	Integrated desktop, mobile, and remote policies define and enforce policies that apply to a given agency entity independent of its location.	If agency policy permits users to work from branch office locations or the agency campus, the agency should ensure that user policies apply independently of their work location. Some policies may be most effectively enforced at the service or data level.

Capability	Description	Use Case Guidance
User Awareness Training	User awareness and training entails that all users be informed of their roles and responsibilities and that appropriate cybersecurity education is provisioned to enable users to perform their duties in a secure manner.	Agencies should understand any differences between the workflows and processes at branch offices and ensure that user trainings account for those differences. Additionally, agencies may consider developing trainings that are specific to a branch office, but they should update the training offerings regularly as changes occur at both the branch office and the enterprise levels.
Supply Chain Risk Management	Supply chain risk management involves (1) implementing a systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and (2) developing risk response strategies for the risks presented by the supplier, the supplied products and services, or the supply chain.	Agencies may develop different processes and workflows for obtaining products and services at branch office locations and may use different suppliers based on mission need or geographic location, for example. Agencies may need to update their supply chain risk management processes to account for any differences between the branch office and the traditional enterprise.
Resource Lifecycle Management	Resource lifecycle management is the end-to-end process of managing resources from development to operation to retirement, such that resources are provisioned and decommissioned in conjunction with the applications they support.	Agencies may have different processes and workflows for lifecycle management for resources at branch office locations compared to those at the traditional enterprise. Where resources are transferred between branch office locations or between branch offices and the traditional enterprise, agencies will need to understand any differences to ensure an appropriate transition.
Security Test and Exercise	Security tests (e.g., penetration testing or red teaming) verify the extent to which a system resists active attempts to compromise its security. Security exercises are simulations of emergencies that validate and identify gaps in plans and procedures.	Agencies should perform regular security test and exercise routines that include branch offices. These could include tests that cover the entire agency, including one or more branch offices, but they should also include tests that are applicable for specific branch offices and account

Capability	Description	Use Case Guidance
		for differences in their threats and environments.
Continuous Monitoring Reporting	Continuous monitoring reporting entails the maintenance of ongoing awareness of informational security, vulnerabilities, and threats to support organizational risk management decisions.	Agencies should ensure that the branch offices are providing sufficient information to enable an accurate understanding of any differences between the branch office and the traditional enterprise. These include differences in the users, roles, workflows, processes, environments, physical protections, and cyber protections, as well as differences in the types of threats to and vulnerabilities at the branch office. Agencies should account for these differences to ensure that they have a holistic view of enterprise-wide risk. Agencies should understand and work to mitigate any limits to their visibility into branch offices, including in circumstances where they lose connectivity with branch offices.
Governance and Policy Auditing	Governance and policy auditing entails validating the proper definition, application, and enforcement of agency rules and policies.	With potential differences due to the roles and responsibilities, users, sizes, and locations of the branch offices, agencies should review their rules and policies to ensure the relevance, compliance, and enforcement for each branch office and should account for these differences when adopting new rules or policies. Additionally, agencies should regularly review these rules and policies to ensure continued applicability and alignment with the branch offices as changes occur in the enterprise and the branch offices.

7.2 POLICY ENFORCEMENT POINT SECURITY CAPABILITIES

PEP security capabilities focus on the network-level and inform technical implementation for a given use case, like branch office communication with agency-sanctioned CSPs. Agencies have the discretion to determine the applicability and level of rigor necessary for applying PEP security

capabilities based on their branch office use, the policy enforcement options available, federal guidelines, and risk tolerance. Specific guidance for agencies to consider when implementing each security capability in the context of the branch office may be provided in the subsequent tables. From the Security Capabilities Catalog, the PEP security capability groups applicable to the Branch Office Use Case correspond to the following security functions:

- Files,
- Web,
- Networking,
- Resiliency,
- DNS,
- Intrusion Detection,
- Enterprise,
- Data Protection, and
- Identity

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

Security capabilities that are not applicable to this use case are listed at the beginning of Section 7. The PEP security capability listing is not exhaustive. Additional security capabilities may be deployed by agencies to reflect their risk tolerances, early adoption of security capabilities, the maturity level of existing cyber programs, etc.

7.2.1 Files PEP Security Capabilities

Branch office environments should receive file protections commensurate with those provided on the agency campus. The agency can deploy services at the branch office location for full-file analysis or may perform some subset of file hygiene tasks at the branch office and depend upon centralized services for full-feature protections. However, if centralized services are employed, precautions should be taken to ensure adequate protections are in place if the branch office loses connectivity to the centralized services. File protections may need to be tuned for the branch offices as these locations may have unique file types that should have their file protections aligned to those roles.

Table 4: Files PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	No specific guidance for this capability.
Content Disarm and Reconstruction	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	No specific guidance for this capability.
Detonation Chamber	Detonation chambers facilitate the detection of malicious code using	No specific guidance for this capability.

Capability	Description	Use Case Specific Guidance
	protected and isolated execution environments to analyze the files.	
Data Loss Prevention	Data loss prevention (DLP) technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	DLP solutions, at both the agency campus and the branch office, should consider any possibilities for file exfiltration from the agency campus through the branch office, and from the branch office, through the agency campus.

7.2.2 Web PEP Security Capabilities

Agencies should, if possible, apply web capabilities commensurate to those available from the agency campus to all data flows from the branch office containing web traffic. Beyond accessing web resources, these data flows could also include access to CSPs, whether agency-sanctioned or not.

Branch locations may have specialized roles that permit a more granular approach to the enforcement of web protections. When accessing agency-sanctioned web-based services, agencies may need to bypass certain protections for functional, performance, or other reasons. In these scenarios, the agency should ensure that compensating protections are in place to mitigate the risks of bypassing protections.

The protections provided to a branch office may need to be augmented for the specific threats or environment of the branch office.

Table 5: Web PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Break and Inspect	Break and Inspect systems, or encryption proxies, terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.	To mitigate the effects of a compromise of the branch office, Break and Inspect solutions deployed to the branch office should, if possible, employ different certificate chains than those in the agency campus and have as short a time to live as is feasible. Break and Inspect solutions should be considered in the context of the sensitivity of data being scanned, the trust level designation of the source and destination, other security capabilities that offer comparable visibility, and the protocols and services in use.

Capability	Description	Use Case Specific Guidance
Active Content Mitigation	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	No specific guidance for this capability.
Certificate Denylisting	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	No specific guidance for this capability.
Content Filtering	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	No specific guidance for this capability.
Authenticated Proxy	Authenticated proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	Security patterns using a CASB or other SECaaS offering should ensure branch office users are authenticated before providing services.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	DLP solutions, at both the agency campus and the branch office, should consider any possibilities for file exfiltration from the agency campus through the branch office and from the branch office through the agency.
Domain Resolution Filtering	Domain resolution filtering prevents entities from using unauthorized DNS resolution services over the DNS-over-Hypertext Transfer Protocol Secure (HTTPS) domain resolution protocol.	No specific guidance for this capability.
Protocol Compliance Enforcement	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, like those documented by the Internet Engineering Task Force (IETF).[8]	No specific guidance for this capability.

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

Capability	Description	Use Case Specific Guidance
Domain Category Filtering	Domain category filtering technologies allow for classes of domains (e.g., banking, medical) to receive a different set of security protections.	No specific guidance for this capability.
Domain Reputation Filtering	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	No specific guidance for this capability.
Bandwidth Control	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	Branch office locations may also have a reduced link capacity, increasing the importance of managed utilization.
Malicious Content Filtering	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	No specific guidance for this capability.
Access Control	Access control technologies allow an agency to define policies that limit what actions may be performed by connected users and entities.	No specific guidance for this capability.

7.2.3 Networking PEP Security Capabilities

Agency branch offices are often dependent on their ability to access agency networks, services, or cloud environments. Connectivity from branch locations to other environments should employ all feasible security mechanisms. As traffic forwarding decisions are foundational to protections, agencies should ensure data flows are forwarded to appropriate destinations and that decision points for making this determination are not easily bypassed or manipulated. Agencies consider the potential reduction in device complexity, capacity, and capability when making determinations about policy enforcement at the branch location. If multiple methods of conveyance are employed (e.g., redundant links, SD-WAN, etc.), care should be taken to ensure policy enforcement parity and situational awareness are maintained.

Table 6: Networking PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Access Control	Access control protections prevent the ingress, egress, or transmission of unauthorized network traffic.	Branch office locations may have reduced physical protections, increasing the importance of device-level validation checks before

Capability	Description	Use Case Specific Guidance
		allowing a device, or its traffic, onto the network.
Internet Address Denylisting	Internet address denylisting protections prevent the ingest or transiting of traffic received from, or destined, to a denylisted internet address.	No specific guidance for this capability.
Host Containment	Host containment protections enable a network to revoke or quarantine a host's access to the network.	Branch office locations may have reduced ability to quickly respond and quarantine physical endpoints, increasing the importance of network-level revocation of device access.
Network Segmentation	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	When VPNs, or similar technologies, are used to bridge branch office networks with other environments, the agency should ensure, if possible, that the bridged networks are segmented so that least privilege access is maintained, and to limit the scope of a compromise of any environment. Agencies may assume the branch office has a higher likelihood of being compromised and should segment the agency campus network and agency CSP services to limit the impact of the compromise of a branch office. If the agency branch office employs a guest network, it should be isolated by physical means, if possible, from the branch office network as well as any connections to external environments. The guest network should utilize as few shared components with the branch office network as is feasible.
Micro segmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data	For branch offices where access to agency services or data may bypass the traditional campus security infrastructure, agencies should

Capability	Description	Use Case Specific Guidance
	workflows, facilitating security controls to protect the data.	consider microsegmentation to more effectively limit the branch office users to the services and data they need, and to mitigate the impact of a compromise of the branch office.

7.2.4 Resiliency PEP Security Capabilities

With differing sizes, locations, and roles, branch office locations often have substantially different resiliency requirements compared to agency campuses. Agencies should work to ensure resiliency protections consider branch office access to the authorized CSPs as well as access to the agency campus, especially if protections covering the branch office are deployed remotely from the branch office.

Table 7: Resiliency PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Distributed Denial of Service Protections	Distributed Denial of Service (DDoS) protections mitigate the effects of distributed denial of service attacks.	As branch office locations are more likely to need access to agency services and data hosted externally to the branch office and are more likely to have a reduced link capacity, DDoS protections can be vital to branch offices. The protections may need to apply to both the agency campus and the branch office, as disruptions to either can impact the branch office. If branch office locations have different methods of connecting to authorized CSPs compared to agency campuses, agencies may need to make changes to DDoS protections protecting CSP environments.
Regional Delivery	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	If branch office locations are in different regions than the agency campus, they may benefit from regional delivery more tailored to their location. If regional delivery options are employed, DDoS and other protections may need to account for these new deployment options.

7.2.5 Domain Name System PEP Security Capabilities

To ensure consistency among agency locations, agencies may have branch office locations leverage the same name resolution services as the agency campus, when possible. However, routing DNS traffic through the agency campus may cause performance issues, especially for branch locations located in remote locations. If the performance problems cannot be ameliorated for a branch location, agencies may consider having the branch office use different name resolution services. If a branch office location uses different name resolution services than the agency campus, the agency should protect name resolution from attack, including the use of DNSSEC to ensure that names are being properly resolved, and, if available, DNS sinkholing to ensure that branch office users do not resolve and contact malicious domains.

Table 8: Domain Name System PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Domain Name Sinkholing	Domain name sinkholing protections are a form of denylisting that protects clients from accessing malicious domains by responding to DNS queries for those domains.	If DNS sinkholing is not deployed, other mechanisms (e.g., intrusion detection and prevention system, web application firewalls (WAFs), etc.) should be utilized to ensure that agency users are protected from accessing malicious domains.
Domain Name Verification for Agency Clients	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to DNSSEC.	No specific guidance for this capability.
Domain Name Monitoring	Domain name monitoring allows agencies to discover the creation of or changes to agency domains.	Agencies may need to update their enterprise domain name monitoring solution to integrate monitoring for branch office domains.
CISA's Protective DNS Service	CISA's Protective DNS Service is a shared service offering that provides domain name sinkholing protections.	If Protective DNS protections need to be augmented or bypassed, the agency should work with CISA[9] to ensure the preservation of commensurate protections and telemetry.

[9] QSMO@cisa.dhs.gov

7.2.6 Intrusion Detection PEP Security Capabilities

Branch offices commonly have fewer physical protections, fewer resources available for protection, and a smaller user base, so their requirements often differ from traditional on-campus environments. Branch offices are also often less integrated with and understood by the NOC or SOC services of the agency campus, especially when a physical presence is required, like obtaining a device for performing post-event forensics. These differences can affect how agencies design and deploy intrusion detection and prevention infrastructure.

Table 9: Intrusion Detection PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Endpoint Detection and Response	Endpoint detection and response (EDR) tools combine endpoint and network event data to aid in the detection of malicious activity.	Agencies should consider relying more on endpoint validation to provide confidence in the endpoints at the branch office, especially when accessing agency services and data.
Intrusion Detection and Prevention Systems	Intrusion detection systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity.	Branch locations may have specialized roles that permit a more granular approach to enforcement of intrusion detection and prevention system protections. For branch offices where connections to remote resources bypass the traditional campus security infrastructure, intrusion detection, and prevention techniques may need to be handled differently, especially if the branch office has more limited resources available to it.
Adaptive Access Control	Adaptive access control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	The branch office may have unique operating hours or other restrictions permitting a more rigorous access control policy. Access control rules may need to be augmented to consider endpoint validation checks. Access control rules may need to consider the users who might work out of a given branch location to limit the exposure of compromised accounts.

Capability	Description	Use Case Specific Guidance
Network Detection and Response	Network detection and response involves the collection and analysis of network event data to aid in the detection and remediation of malicious activity.	Agencies should consider opportunities to deploy network detection and response capabilities within branch offices. Agencies may also consider other methods to obtain detection or visibility. For example, an agency might consider routing branch office traffic through specific external sensor locations that provide visibility. Alternatively, an agency might obtain visibility from agency services and infrastructure hosted outside the branch office (e.g., proxies, agency web services, SECaaS).

7.2.7 Enterprise PEP Security Capabilities

Agency branch offices are often dependent on their ability to access agency networks, services, or cloud environments. There are numerous methods for connecting, most commonly VPNs; each of which can provide a wealth of access to agency internal services. Branch office locations will often make these connections via the internet, necessitating extra care to ensure that these entry points are well-secured. To mitigate the opportunity for and impact of credential theft, these services should only be available using secure protocols (e.g., IP Security (IPsec), TLS) and should use MFA.

Table 10: Enterprise PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Security Orchestration, Automation, and Response	Security Orchestration, Automation, and Response (SOAR) tools define, prioritize, and automate the response to security incidents.	When integrating branch office locations into existing SOAR solutions, agencies should account for how the loss of connectivity from the branch office to the agency campus or authorized CSPs might affect automatic responses in the branch office.
Shadow Information Technology Detection	Shadow information technology (IT) detection systems detect the presence of unauthorized software and systems in use by an agency.	Agency-sanctioned CSP services should be differentiated and permitted in a manner such that unsanctioned services from the same CSP are not accessed in the same manner as sanctioned CSP services.

Capability	Description	Use Case Specific Guidance
Virtual Private Network	VPN solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	The branch office, or individual branch office entities, may use a VPN into the campus network, or to agency environments in CSPs. Given the access to internal services that VPNs can provide along with the need to make them available to users connecting from the branch office, these entry points need to be well-secured, including being up to date with security patches. VPN services can be used to provide bulk data encryption for multiple branch office entities, enabling consistent traffic forwarding policies. If multiple methods of conveyance are employed (e.g., redundant links, SD-WAN, etc.), care should be taken to ensure consistent VPN policies are applied across all conveyance paths.

7.2.8 Data Protection PEP Security Capabilities

When designing and deploying data protections, agencies should consider the data protection needs of branch office locations, which may differ from agency campuses. To facilitate common understanding and practices for protecting data, the data protections employed by an agency should be uniform across all agency locations, if possible. If different protections are employed at a branch office as compared to other locations, agencies need to ensure that users, as well as the NOC and SOC teams, understand these differences to avoid the application of the wrong protections at a location.

Table 11: Data Protection PEP Security Capabilities

Capability	Description	Use Case Specific Guidance
Access Control	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	No specific guidance for this capability.
Protections for Data at Rest	Data protection at rest aims to secure data stored on any device or storage medium.	Branch offices may have less in the way of physical protections than an agency campus, increasing the need for protections for data stored on devices at the branch office.

Capability	Description	Use Case Specific Guidance
Protections for Data in Transit	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	With the need to communicate agency data between the branch office and the agency campus, coupled with possibly decreased physical protections at the branch office, protections for data in transit are paramount. These strong data protections should combine identity guarantees of the recipient and validation of the endpoint receiving the data.
Data Loss Prevention	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	DLP solutions, at both the agency campus and the branch office, should consider any possibilities for file exfiltration from the agency campus through the branch office, and from the branch office through the agency campus.
Data Access and Use Telemetry	Data access and use telemetry identifies agency-sensitive data stored, processed, or transmitted, including those located at a service provider, and enforcing detailed logging for access or changes to sensitive data.	As part of an overall DLP program, the agency should track the data accessed or transmitted to the branch office. The agency should monitor users accessing data from the branch office to validate that they should be accessing data from the branch office and to look for discrepancies or changes in their data access patterns.
Data Labeling	Data labeling is the process of tagging data by categories in order to protect and control the use of data and identify a level of risk associated with the data.	Agencies should ensure that data labeling policies are applied by branch offices and account for any potential differences in the workflows, processes, or environment of a branch office.
Data Inventory	Data inventory entails developing, documenting, and maintaining a current inventory of agency data.	Agency data inventories should track data that is stored at or accessed from branch offices, including data accesses for data stored in the agency campuses, other branch offices, and agency cloud environments.

7.2.9 Identity PEP Security Capabilities

Agencies should manage their identities in a centralized manner to ensure enterprise visibility into the branch office identities as well as to facilitate user mobility between agency locations. As branch offices may lose connectivity to the main campuses, agency should understand and mitigate the effect of disconnected operation on their authentication and user management processes. Agencies may consider the use of federated identities, Identity-as-a-Service and other identity management techniques to facilitate the branch office use of cloud and other external resources. Table 12 lists the applicable Identity PEP Security Capabilities for the Branch Office Use Case.

Table 12: Identity PEP Security Capabilities

Capability	Description	Use Case Guidance
Adaptive Authentication	Adaptive authentication aligns the strength of the user or entity authentication mechanisms to the level of risk associated with the requested authorization.	Agencies should consider adaptive authentication solutions that can account for differences in workflows, processes, environments, or risks in branch offices.
Entitlement Inventory	Entitlement inventory entails developing, documenting, and maintaining a current inventory of user and entity permissions and authorizations to agency resources.	Agencies may need to update their entitlement inventory to include branch office users and entities as well as any permissions and authorizations that are specific to any branch office.
Secrets Management	Secrets management entails developing and using a formal process to securely track and manage digital authentication credentials, including certificates, passwords, and Application Programming Interface (API) keys.	Agencies may need to update their processes for managing secrets to account for secrets that are created or used by the branch office. As branch offices may lose connectivity to the agency campus or authorized CSPs, agencies should understand how the loss of connectivity can affect secrets management at branch offices, including how it might affect their response and recovery from malicious or damaging events.
Behavioral Baselining	Behavioral baselining is capturing information about user and entity behavior to enable dynamic threat discovery and facilitate vulnerability management.	Behavioral baselining should track the branch office use of agency services or data, and it should account for potential behavioral differences for branch office employees operating outside the branch office location or non-branch office employees using the branch office location.

Capability	Description	Use Case Guidance
Enterprise Identity, Credential, and Access Management	Enterprise ICAM entails maintaining visibility into agency identities across agency environments and managing changes to those identities through a formal (preferably automated) process.	Agency enterprise identity and access management solutions should integrate visibility and identity lifecycle management for branch office users and entities, including accounting for how the loss of connectivity from the branch office to the agency campus or authorized CSPs might affect the visibility or identity lifecycle management.
Multi-factor Authentication	MFA entails using two or more factors to verify user or entity identity.	Agencies should, wherever possible, employ phishing-resistant MFA[10] as part of verifying identity, including re-verification of identity when users or entities seek to perform suspicious or sensitive actions. This will allow agencies to minimize opportunities for lateral movement or privilege escalation from account compromise. Where MFA is used at branch offices, the authentication processes should account for situations where the branch office loses connectivity to centralized services.
Continuous Authentication	Continuous authentication entails validating and re-authenticating identity through the lifecycle of entity interactions.	No specific guidance.

[10] "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," Office of Management and Budget M-22-09 (2022). https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

8. TELEMETRY REQUIREMENTS

As agencies transition to branch offices connecting directly to external services, visibility by CISA must be preserved through information sharing. Figure 7 shows the conceptual architecture of the Branch Office Use Case, with the telemetry requirements added as lines on certain data flows.

These lines, depicted in Figure 7, indicate when an agency must share telemetry with CISA.

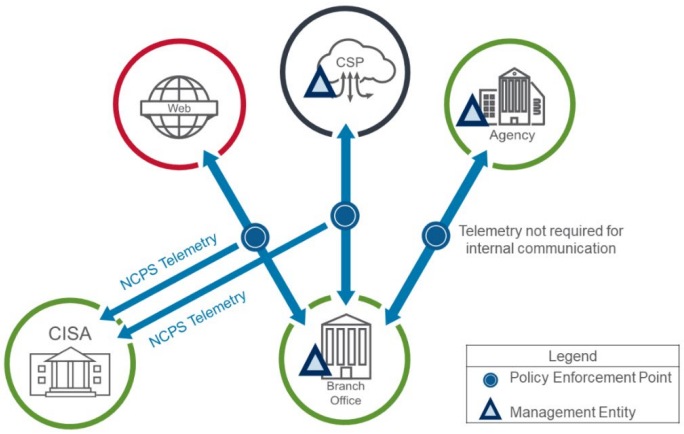

Figure 7: Branch Office Telemetry Sharing with CISA

Figure 7 further 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 applicable to the data flows between the branch office and the web and any CSPs. Consult the NCPS program[11] and CDM program[12] for further details.

Agencies should work with the NCPS program and the CDM program to maintain appropriate visibility for the branch office.

9. CONCLUSION

The Branch Office Use Case defines how network and multi-boundary security should be applied when an agency conducts work in more than one physical location, in which most of the IT services are provided by another branch office rather than the agency campus. This document provides guidance on how an agency can configure its branch office data flows and apply relevant TIC security capabilities. It considers three network security patterns:

- Secure branch office access to agency-sanctioned CSPs,
- Secure branch office access to web, and
- Secure branch office access to agency campus.

This use case document should be used in conjunction with the Security Capabilities Catalog and any TIC overlays that are applicable to service providers that an agency employs.

[11] "National Cybersecurity Protection System (NCPS)," https://www.cisa.gov/national-cybersecurity-protection-system-ncps.
[12] "Continuous Diagnostics and Mitigation (CDM)," https://www.cisa.gov/cdm.

APPENDIX A – GLOSSARY AND DEFINITIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

APPENDIX B – RELATED FEDERAL GUIDELINES

The following list of documents include the most recent version of the guidance documents available at the time of this publication, including drafts.

Cybersecurity and Infrastructure Security Agency, *Capacity Enhancement Guides for Federal Agencies: Implementing Strong Authentication*, October 2020.

Cybersecurity and Infrastructure Security Agency, *Cloud Security Technical Reference Architecture, Version 2.0*, June 2022.

Cybersecurity and Infrastructure Security Agency, *Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*, November 2021.

Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model, Version 2.0*, April 2023.

Department of Defense, *Zero Trust Reference Architecture, Version 2.0*, July 2022.

Cybersecurity and Infrastructure Security Agency *Extensible Visibility Reference Framework Guidebook Request for Comment Draft*, April 2022.

Federal Information Security Modernization Act of 2014 (Public Law 113-283), codified in relevant part in 44 U.S.C. §§ 3551-8.

National Institute of Standards and Technology Special Publication, 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, December 2020.

National Institute of Standards and Technology Special Publication, 800-63-3, Digital Identity Guidelines, March 2020.

National Institute of Standards and Technology, Special Publication 800-207, Revision 1, Zero Trust Architecture, August 2020.

National Institute of Standards and Technology, Special Publication 800-210, General Access Control Guidance for Cloud Systems, July 2020.

Cybersecurity and Infrastructure Security Agency, Secure Cloud Business Applications Microsoft 365 Baselines, Draft December 2022.

Cybersecurity and Infrastructure Security Agency, Secure Cloud Business Applications Technical Architecture Request for Comment Draft, April 2022.