Trusted Internet Connections 3.0

Pilot Process Handbook

October 2021

Version 1.0

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

Version	Date	Revision Description	Sections/Pages Affected
Draft	December 2019	Initial Release	All
1.0	October 2021	Updated Pilot Conclusion Process	Pg. 5
		Clarified Use Case Definition	Pgs. 5-6
		Updated Use Case Approval	Pg. 7

TIC 3.0 Pilot Process Handbook

Table of Contents

1. Introduction 1
2. Purpose of the Pilot Process Handbook 1
3. Scope and Key Stakeholders 1
4. Expectations and Outcomes 2
5. Pilot Process 2
   5.1 Proposal Development and Submittal 3
   5.2 Proposal Review and Approval 3
   5.3 Project Plan Development and Submittal 4
   5.4 Project Plan Review 4
   5.5 Pilot Execution and Management 4
   5.6 Pilot Conclusion 5
   5.7 Use Case Development 5
   5.8 Use Case Approval 7
   5.9 Acquisitions 7
   5.10 Continuing Feedback 8
   5.11 Compliance Process 8
6. Timeline 9
7. Roles and Responsibilities 10
Appendix A – Glossary and Definitions 11

List of Figures

Figure 1: TIC Pilot Process 2
Figure 2: Agency-Initiated Proposal Phase 3
Figure 3: Vendor-Initiated Proposal Phase 3
Figure 4: Proposal Review and Approval Phase 3
Figure 5: Project Plan Development and Submittal Phase 4
Figure 6: Project Plan Approval Phase 4
Figure 7: Pilot Execution and Management Phase 4
Figure 8: Pilot Conclusion Phase 5
Figure 9: Use Case Development Phase 6
Figure 11: Use Case Approval Phase 7
Figure 12: Acquisitions 7
Figure 13: Continuing Feedback Phase 8
Figure 14: Compliance Process 8

List of Tables

Table 1: Revision History ii
Table 1: Notional TIC Pilot Timeline 9

1. Introduction

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

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

2. Purpose of the Pilot Process Handbook

The purpose of this document is to describe the process by which pilots will be conducted by agencies in accordance with OMB Memorandum M-19-26. While federal standards and requirements define what to secure across an entire enterprise, TIC 3.0 focuses on securing different types of environments, including cloud and mobile environments, along with connections between agencies and selected partners. To provide useable guidance in securing the connections, the cloud, and the mobile users, TIC pilots will use real world implementation test cases to identify solutions for securing new types of environments. CISA will update relevant security policies and architectures to enable agencies to focus on both network and data-level security and privacy, while ensuring incident detection and prevention capabilities are modernized to address the latest threats.

A pilot program is a small-scale, short-term experiment that assesses the feasibility and utility of a program in an organization. TIC pilots follow this framework to reveal insights into different methodologies for implementing the TIC security capabilities.

3. Scope and Key Stakeholders

This document outlines the sequence of steps that agencies, vendors, and key stakeholders should conduct for a successful TIC pilot: proposal development and submittal, proposal approval, project plan submittal and approval, pilot execution and management, pilot conclusion, and use case development. Some pilots may require additional steps based on the unique circumstances of the piloting agency.

Audience:

- Federal executive civilian agencies
- Vendors

Key Stakeholders:

- OMB
- CISA
- GSA
- Federal Chief Information Security Officer (CISO) Council TIC Subcommittee

[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.

4. Expectations and Outcomes

To ensure the success of the TIC program, CISA is seeking agencies to actively participate in pilots. A pilot should test the configuration and security capabilities of a technology in an agency's environment. Each pilot is expected to:

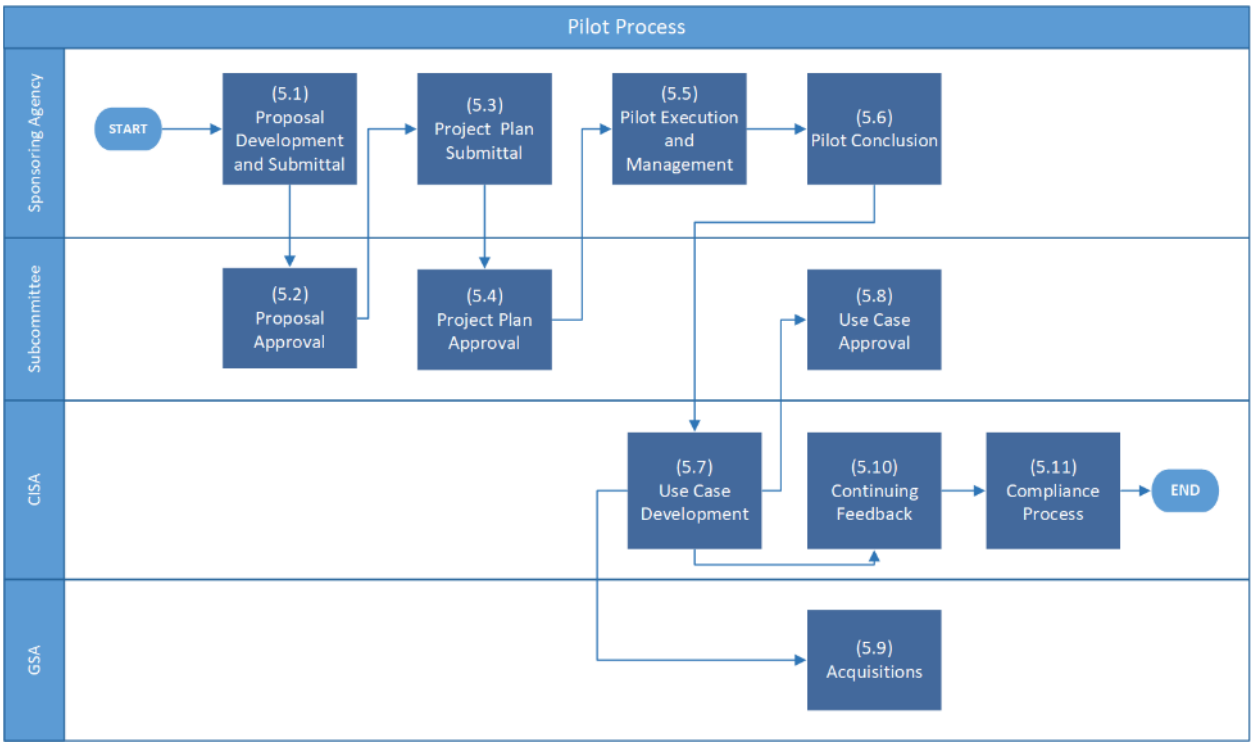
- Address technology that can be used by the broader Federal Government
- Identify applicable security capabilities to secure their environments
- Explain how the applicable security capabilities requirements are met
- Follow a defined and structured timeline
- Be carefully considered and planned
- Be supported by agency leadership

Upon completion of a pilot, CISA will collect and analyze lessons learned from the sponsoring agency. The outcome can be used to develop new, and augment existing use cases.

5. Pilot Process

The piloting process is a collaborative and iterative process that ensures consistency in the execution of each pilot. Sponsoring agencies are the primary executors of this process, while other key stakeholders, such as OMB, CISA, GSA, and the Federal CISO Council TIC Subcommittee (hereinafter referred to as the "Subcommittee"), will review submissions, provide feedback and offer ongoing support in accordance with OMB Memorandum M-19-26. This process consists of eleven phases as depicted in Figure 1 below.

Figure 1: TIC Pilot Process

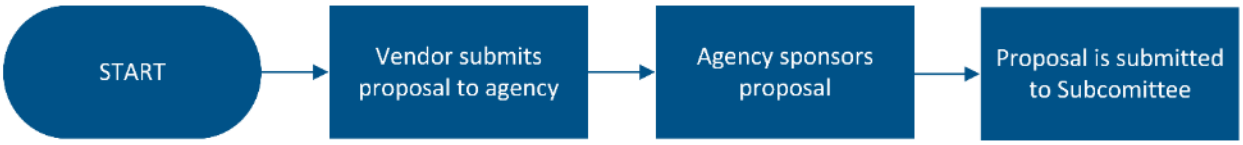


5.1 Proposal Development and Submittal

The pilot process begins with an agency, or a vendor, developing a proposal that:

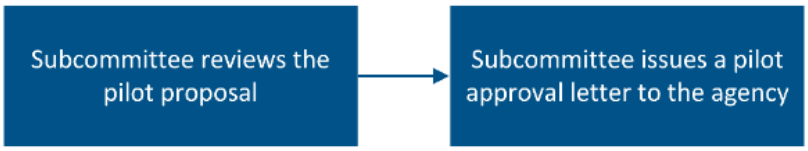
- Describes the goals and desired outcomes of the pilot
- Identifies proposed technologies, processes, and resources to perform the pilot
- Confirms that resources will be prioritized to complete the pilot, including submission of all required artifacts
- Secures participation from the relevant and associated vendors
- Demonstrates how this pilot can be used by the broader spectrum of federal agencies

The Subcommittee will periodically open a solicitation window to receive proposals for new pilots. CISA will provide material (i.e. templates or guides) to guide agencies and vendors in developing a proposal to submit to the Subcommittee. Agencies and vendors can both submit a pilot proposal. However, vendors are expected to obtain agency sponsorship prior to submitting their pilot proposals to the Subcommittee.



5.2 Proposal Review and Approval

This phase determines if the proposal will become a pilot. The Subcommittee reviews the proposal with key stakeholders, assessing the relevance of the pilot to the TIC strategic program goals and, if acceptable, approves the pilot.



5.2.1 Subcommittee Review

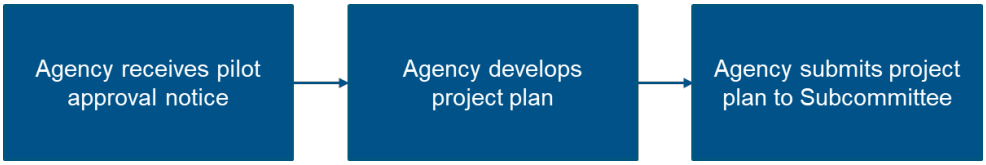
The Subcommittee leads a review of the proposal with key stakeholders, including OMB, CISA, and GSA.

5.2.2 Subcommittee Approval

The Subcommittee issues a pilot approval letter to the agency once the proposal is approved.

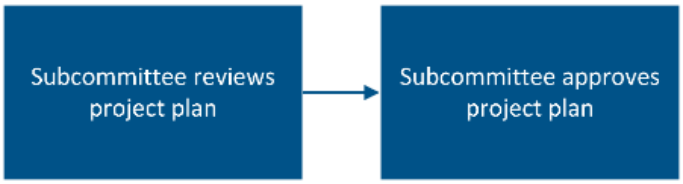
5.3 Project Plan Development and Submittal

Once the pilot is approved, the pilot proceeds to the project plan phase. The agency develops a project plan that includes the pilot's schedule, deliverables and desired outcomes. Project plans details may include general project activities, such as identifying security tools, selecting security requirements, test planning, and pilot closeout. The project plan is then submitted to the Subcommittee for initial review.



5.4 Project Plan Review

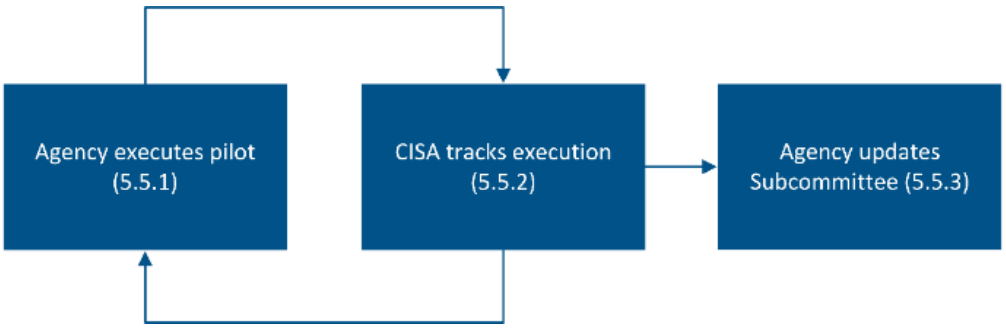
The Subcommittee reviews the project plan with CISA and GSA for feasibility. CISA will work with the sponsoring agency to make any adjustments, if needed, to the project plan. Upon approval, the project plan moves into the pilot execution and management phase.



5.5 Pilot Execution and Management

The pilot execution and management phase marks the beginning of the pilot. CISA, in coordination with OMB, GSA, and the Subcommittee, will track the agency TIC pilot's execution and management. This phase is cyclical in nature in which the agency executes the pilot while stakeholders observe the execution to ensure the schedule, deliverables and desired outcomes are met.

Figure 7: Pilot Execution and Management Phase



5.5.1 Agency Executes Pilot

The agency executes the pilot and is responsible for providing CISA and the Subcommittee with regular updates on the progress and status of the pilot. CISA and the Subcommittee will provide guidance as needed.

5.5.2 CISA Tracks Execution

CISA, in coordination with OMB and GSA, tracks the agency's execution of the pilot. CISA tracks the pilot's progress and risks to ensure the pilot stays on schedule. CISA also distills lessons learned from the pilots to develop TIC use cases.

5.5.3 Agency Updates Subcommittee

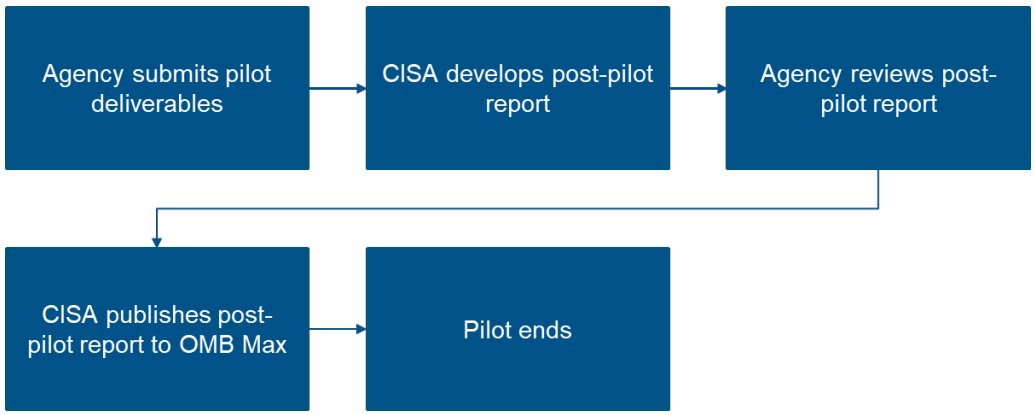
The agency that submitted the pilot provides regular updates to the Subcommittee in coordination with CISA. The updates will include the pilot's progress, risks, and opportunities for government-wide collaboration. Updates are typically provided every two weeks, i.e. bi-weekly.

5.6 Pilot Conclusion

Once a pilot has concluded, the agency must submit the following deliverables:

- Lessons learned
- Capability mapping

CISA will provide guidance and resources, as needed, for completing the deliverables. Following the completion of a pilot, CISA will author a post-pilot report to ensure consistent tone and detail across agencies. The post-pilot reports will become available as a resource to other agencies via OMB Max. Piloting agencies will review the post-pilot report prior to publication on OMB Max.



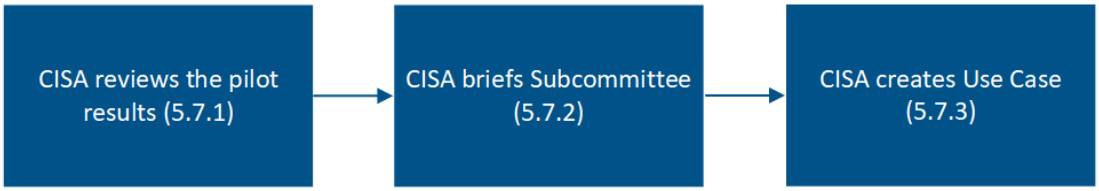
5.7 Use Case Development

TIC use cases provide guidance on the secure implementation of 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. Use cases build upon the key concepts 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).

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.

The Reference Architecture, Security Capabilities Handbook, and Use Case Handbook should be used in conjunction with this document and the use case template when developing use cases.



5.7.1 CISA Reviews the Pilot Results

CISA, in coordination with the pilot agency and GSA, assesses the results of the pilot and determines how outcomes can be used to update TIC use case guidance. If CISA determines the pilot does not meet the requirements needed to create or update a use case, then CISA will brief the Subcommittee as to why the pilot did not result in a new or updated TIC use case.

5.7.2 CISA Briefs Subcommittee

CISA briefs the Subcommittee on pilot outcomes and suggests updates to TIC use cases. The Subcommittee provides feedback to the pilot agency and CISA regarding the pilot outcomes.

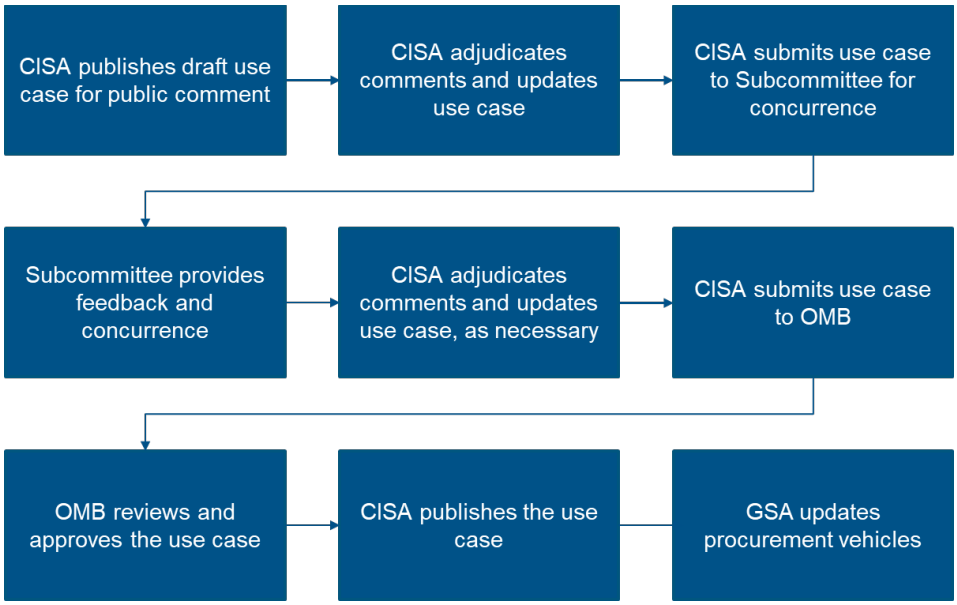
5.7.3 CISA Creates Use Case

CISA, in coordination with the agency, creates a use case based on the pilot, any lessons learned of the pilot submitted by the agency, and Subcommittee feedback.

5.8 Use Case Approval

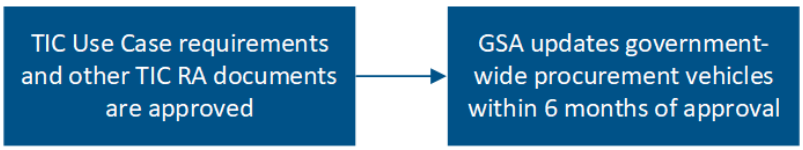
CISA will release the draft use case for public comment to ensure the guidance fully address security considerations related to TIC for the given scenario. Reviewers in the public comment period including OMB, GSA, the Subcommittee, other federal agencies, vendors, trade groups, academia, and more. CISA will adjudicate the comments and submit the updated use case to the Subcommittee for concurrence.

After adjudicating comments from the Subcommittee, CISA submits the use case to OMB for approval. OMB conducts a final review of the use case and approves it for publication. CISA then publishes the finalized use case for agency use and public awareness. All use case updates will be made to GSA procurement vehicles, as appropriate, within six months of approval of the new use case.



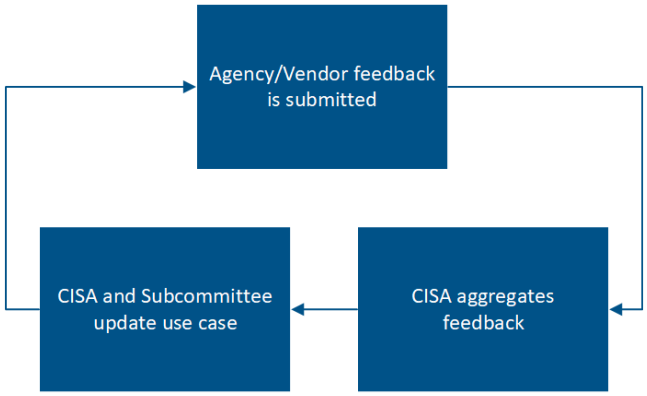
5.9 Acquisitions

GSA will update government-wide procurement vehicles, as appropriate, within six months of the approval of new TIC use case requirements and other TIC reference architecture documentation. The GSA process will not be tracked by CISA, the Federal CISO Council, nor the Subcommittee.



5.10 Continuing Feedback

CISA, in coordination with GSA, will establish a coordinated process for soliciting agency and vendor input on approved TIC use cases and other TIC reference architecture documentation. CISA will keep TIC use cases and other TIC reference architecture documentation up-to-date as changes are approved and as technology improves. Once the use case is approved by the Subcommittee, the use case proceeds into the continuing feedback phase. This phase allows for the repeated evaluation of published use cases to account for advances in technology and implementation optimization. CISA, in coordination with the Subcommittee, continuously reviews and incorporates vendor and agency comments into TIC use cases, as applicable.



5.11 Compliance Process

Within 90 days of the release of each TIC use case, CISA, in coordination with the pilot agency and GSA, will develop a compliance process to validate that agencies are implementing the security controls illustrated by the TIC use cases. CISA will update this process as necessary to promote continuous improvement.

6. Timeline

Multiple stakeholders have authority over various stages of the pilot process. The pace of the pilots relies on timely actions by these stakeholders. Pilot duration will depend on the ability of the agency, OMB. CISA, and the Subcommittee to perform required actions within proposed timelines. The notional timeline represents the standard events that will occur throughout an illustrative 6-month process.

Table 2: Notional TIC Pilot Timeline

Month / Task	1	2	3	4	5	6
Proposal Submittal	X					
Proposal Approval	X					
Project Plan Submittal		X				
Project Plan Approval		X				
Pilot Initiation			X			
Pilot Execution and Management			X	X		
Pilot Conclusion				X		
Use Case Development				X		
Use Case Approval				X	X	
Acquisitions					X	
Continuing Feedback						X
Compliance Verification Process						X

7. Roles and Responsibilities

- Sponsoring Agency
  - Proposal development and submittal
  - Project plan development and submittal
  - Pilot execution and project management
  - Vendor Sponsorship
- Vendor
  - Proposal development
  - Assistance on execution of the pilot
- Federal CISO Council Subcommittee (including OMB)
  - Proposal process management
  - Solicitation of agency participation
  - Ongoing feedback and review of proposals, pilots, use cases, and project plan
  - Approval of proposals, pilots and use cases
- CISA
  - Stakeholders collaboration
  - Pilot execution management
  - Progress tracking
  - Use case creation and document management
  - Ongoing feedback and review of proposals, pilots, use cases, and project plan
  - Post-pilot reports development and submittal
- GSA
  - Procurement vehicle updates

Appendix A – Glossary and Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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