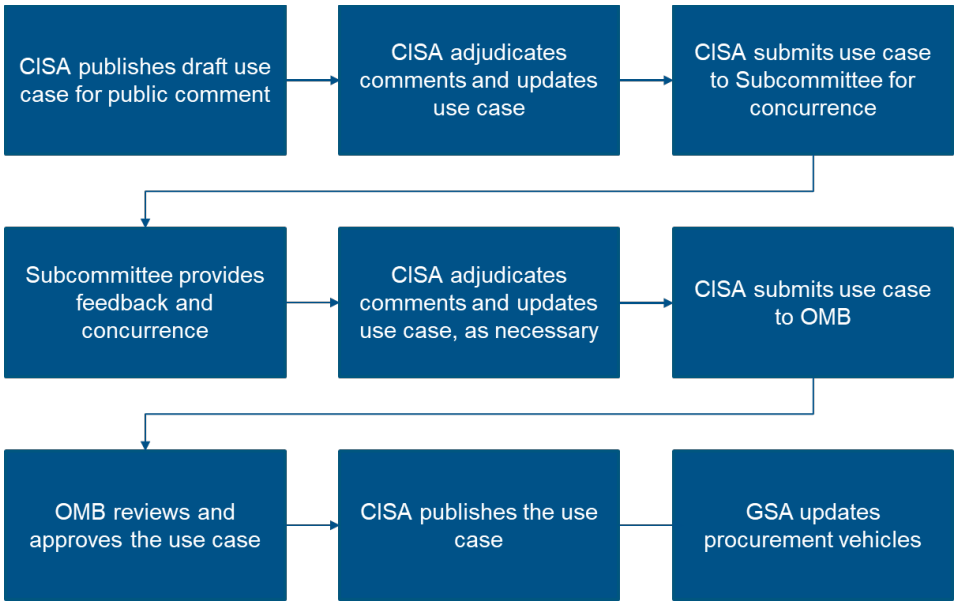
5.8 Use Case Approval

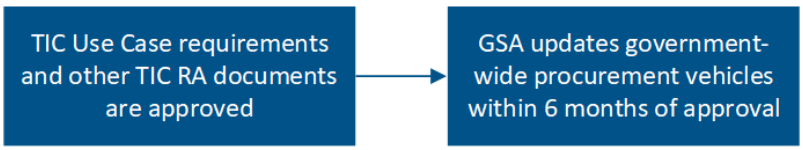
CISA will release the draft use case for public comment to ensure the guidance fully address security considerations related to TIC for the given scenario. Reviewers in the public comment period including OMB, GSA, the Subcommittee, other federal agencies, vendors, trade groups, academia, and more. CISA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



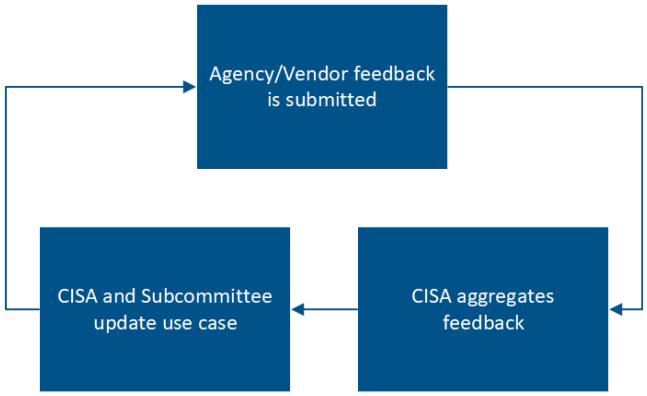
5.9 Acquisitions

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.