Trusted Internet Connections 3.0

TIC Core Guidance Volume 1:

Program Guidebook

July 2020

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	July 2020	Response to RFC Feedback	All

Approved by:

BRYAN S WARE

Digitally signed by BRYAN S WARE
Date: 2020.07.30 13:56:10 -04'00'

Bryan Ware
Assistant Director, Cybersecurity Division

Acknowledgments

The modernization of the Trusted Internet Connections (TIC) initiative is the product of ongoing multi-agency collaboration and supported by resources from several agencies.

Key Stakeholders

- Department of Homeland Security Cybersecurity and Infrastructure Security Agency
- General Services Administration Enterprise Infrastructure Solutions
- General Services Administration Federal Acquisitions Service Office of Information Technology Category
- Federal Chief Information Officers Council
- Federal Chief Information Security Officers Council
- Federal Small Agency Chief Information Officers Council
- Office of the Federal Chief Information Officer
- Office of the Federal Chief Information Security Officer
- National Institute of Standards and Technology

Strategic Contributors

- Royce Allen, Department of Veterans Affairs
- Rose Bernaldo, Department of Commerce
- Patrick Bevill, Federal Retirement Thrift Investment Board
- Mark Bunn, Cybersecurity and Infrastructure Security Agency
- Gerald Caron, Department of State
- Guy Cavallo, Small Business Administration
- Alma Cole, Department of Homeland Security
- Sean Donelan, Industry
- Matt Goodrich, Industry
- Beau Houser, United States Census Bureau
- Jay Huie, Executive Office of the President
- Mark Irvin, Department of the Interior
- Carrie Lee, Department of Veterans Affairs
- Ashley Mahan, General Services Administration
- Rob McKinney, Environmental Protection Agency
- Eric Mill, Individual
- Stu Mitchell, Industry
- Brian Moore, Department of State
- Justin Morgan, General Services Administration
- Sara Mosley, Federal Deposit and Insurance Corporation
- Yu (Boris) Ning, United States Digital Service
- Stuart Ott, Department of the Interior
- Travis Richardson, Department of Health and Human Services
- Maria Roat, Small Business Administration
- Tamia Russell, Office of Management and Budget
- Jim Russo, General Services Administration
- Matt Smith, Department of Homeland Security
- Meria Whitedove, United States Department of Agriculture
- Larry Tun, Department of Justice
- Tim Wang, Office of Management and Budget

TIC Working Group Participants

Table 2: TIC Working Group Participants

Bureau of Economic Analysis	Internal Revenue Service
Consumer Financial Protection Bureau	International Trade Administration
Corporation for National and Community Service	National Aeronautics and Space Administration
Defense Nuclear Facilities Safety Board	National Council on Disability
Department of Commerce	National Endowment for the Arts
Department of Defense	National Endowment for the Humanities
Department of Education	National Labor Relations Board
Department of Energy	National Oceanic and Atmospheric Administration
Department of Health and Human Services	National Science Foundation
Department of Homeland Security	National Transportation Safety Board
Department of Housing and Urban Development	Nuclear Regulatory Commission
Department of Justice	Office of Management and Budget
Department of State	Office of Personnel Management
Department of the Interior	Overseas Private Investment Corporation
Department of the Treasury	Pension Benefit Guaranty Corporation
Department of Transportation	Presidio Trust
Department of Veterans Affairs	Railroad Retirement Board
Environmental Protection Agency	Sandia National Laboratories
Equal Employment Opportunity Commission	Securities and Exchange Commission
Export-Import Bank	Small Business Administration
Farm Credit Administration	Social Security Administration
Federal Election Commission	United States Access Board
Federal Deposit and Insurance Corporation	United States Census Bureau
Federal Mediation and Conciliation Service	United States Commodity Futures Trading Commission
Federal Retirement Thrift Investment Board	United States Customs and Border Protection
Federal Trade Commission	United States Department of Agriculture
General Services Administration	United States Patent and Trademark Office
Inter-American Foundation	United States Trade and Development Agency

Executive Summary

The Trusted Internet Connections (TIC) initiative was established in 2007 by the National Security Presidential Directive (NSPD) 54 and Homeland Security Presidential Directive (HSPD) 23. The Office of Management and Budget (OMB), Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and General Services Administration (GSA) oversee the TIC initiative which originally consolidated federal networks and standardized perimeter security for the federal enterprise.

The TIC initiative has evolved from simply reducing external network connections to protecting agency enterprise perimeters, mobile, and cloud connections with a focus on increasing the use of boundary protection capabilities to protect agency assets from an evolving threat landscape. Over time, greater bandwidth demands, transport encryption, and perimeter services were placed on agency TIC access points beyond their ability to scale. The growing demands on the enterprise perimeter and degraded performance increased the cost and decreased the effectiveness of the TIC initiative when using cloud services.

In 2017, the *Report to the President on Federal Information Technology Modernization* identified the TIC initiative as a barrier to cloud adoption. Removing barriers to modernization is one of the primary goals of the recent update to the TIC policy, TIC 3.0. A key feature of both the report and the policy update is the ability for agencies to conduct cloud and TIC pilots to leverage modern architectures and technology to improve agency information technology (IT) and cybersecurity approaches to protect assets. Results and lessons learned from the TIC pilots will inform the TIC use cases, developed to support the broader use of cloud by agencies. While the policy update provides greater flexibility, agencies will have to carefully consider the risks associated with hosting agency information and applications in the cloud.

Authorities

The TIC initiative was originally derived from the NSPD 54 and HSPD 23. OMB Memorandum (M) 19-26: *Update to the Trusted Internet Connections (TIC) Initiative* was published to update the initiative and provide agencies with increased flexibility to take advantage of advanced capabilities, flexible architectures, and removing barriers to cloud and modern technologies. The TIC initiative is also influenced by other federal authorities that set the groundwork for the TIC initiative.

- Federal Information Security Modernization Act (P.L. 113-283), December 2014.
- Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 2017.
- *Report to the President on Federal Information Technology Modernization*, December 2017.

A list of relevant legislation, policies, directives, regulations, memoranda, standards, and guidelines can be found in Appendix B.

Scope and Audience of the TIC 3.0 Guidance

The scope of the TIC 3.0 guidance encompasses the TIC initiative and other federal program artifacts and publications necessary to explain key elements, goals, and objectives of TIC 3.0. Publications and artifacts may consist of acquisition, technical, and non-technical procedures and policies that are relevant to support the implementation of TIC capabilities at, or on behalf of, federal agencies.

The primary audience of the TIC 3.0 guidance documentation includes federal civilian agencies, contractors, and vendors that align with the TIC initiative. The documents can be leveraged by stakeholders ranging from policy, acquisition, technical, and cybersecurity personnel to agency information technology leadership (e.g., Chief Information Officers (CIOs) and/or Chief Information Security Officers (CISOs)). Non-federal organizations may derive value from the documents as programs, strategies, and approaches are being considered to address multi-boundary or perimeter security needs.

Reader's Guide

The 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 have led up to the latest version of TIC and why those changes have occurred. The documents go into high-level technical detail to describe the exact changes in architecture for TIC 3.0. The documents are additive; each builds on the other like chapters in a book. As depicted in Figure 1, the documents should be referenced in order and to completion to gain a full understanding of the modernized initiative.

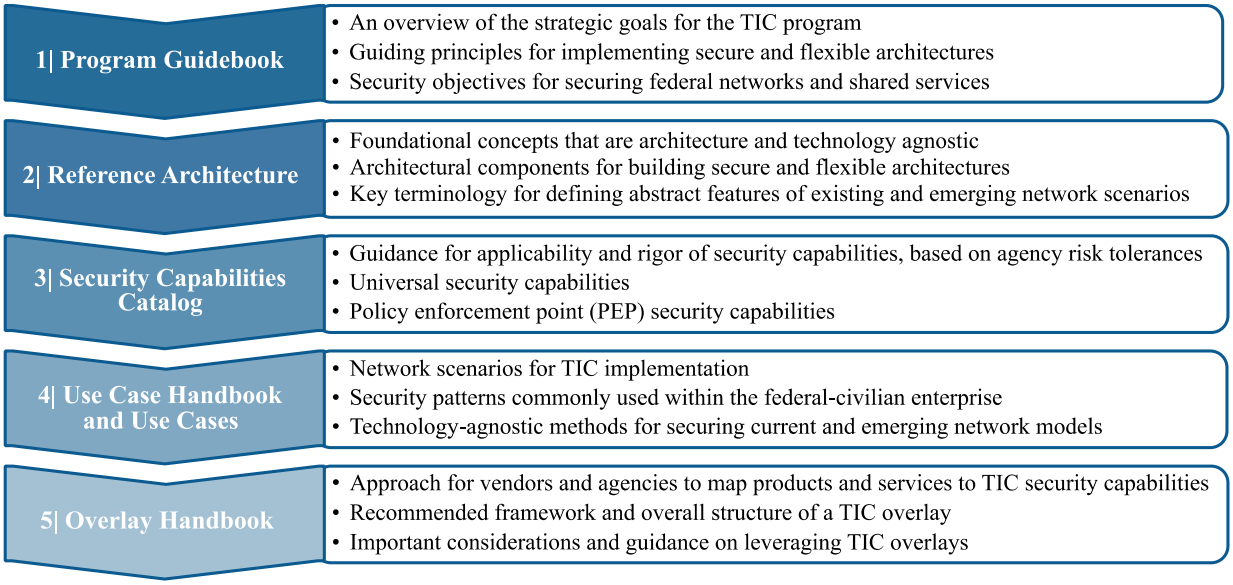

Figure 1: TIC 3.0 Guidance Snapshot

TIC 3.0 Program Guidebook

Table of Contents

List of Figures

List of Tables

1. Introduction

Trusted Internet Connections (TIC), originally established in 2007, is a federal cybersecurity initiative intended to enhance network and 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.

1.1 Key Terms

In an effort to avoid confusion, terms frequently used throughout the TIC 3.0 documentation are defined below. Some of these terms are explained in greater detail throughout the TIC 3.0 guidance. A comprehensive glossary and acronyms list with applicable attributions can be found in Appendix C – 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, hereafter referred to as "Web."

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

[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.

procedures performed by individuals).[2] Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

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.

1.2 Policy Updates and Strategic Changes

Historically, the TIC initiative has established and maintained a federal network security baseline by requiring agencies to consolidate and monitor their external network connections. The past iterations of the initiative focused on securing traffic at the physical agency network perimeter through a traditional TIC access point that operated EINSTEIN[3] sensors, deployed by the National Cybersecurity Protection System (NCPS) program. However, the federal IT landscape has shifted markedly in the decade since the TIC program's initiation, rendering this one-size-fits-all approach, in which all agency network traffic is routed through a limited number of agency-owned or service provider-maintained access points, increasingly unfeasible.

OMB M-19-26 broadens the concepts of the program to accommodate cloud and mobile applications, services, and environments. The updated OMB policy signals a shift in the focus of the TIC initiative from control requirements and compliance towards architecture, strategy, visibility, and flexibility. The program now envisions a flexible perimeter or multi-boundary as compared to the concept of a hard perimeter as previously conceptualized.

The updated OMB policy signals a shift in the focus of the TIC initiative from control requirements and compliance towards architecture, strategy, visibility, and flexibility.

[2] "Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4)," April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[3] "EINSTEIN," Cybersecurity and Infrastructure Security Agency (2019). https://www.cisa.gov/einstein.

Additionally, while the NCPS and TIC initiatives continue to support and complement each other, neither the OMB policy nor the TIC program requires TIC access points and EINSTEIN sensors to be embedded into every type of architecture.

2. Purpose of the Program Guidebook

The *TIC 3.0 Program Guidebook* (Program Guidebook) offers guidance to agencies and vendors that are supporting the TIC initiative. It explains the direction, background, and approaches to implement the modernized initiative. This document guides agencies and vendors through the history of the program, the push for its modernization, and the updated strategy. The guidebook explains:

- The history of the TIC initiative,
- The direction for the program,
- Core updates and changes to the program,
- TIC 3.0 guidance and how to use it,
- The use of TICAPs and MTIPS in the modernization program,
- High-level implementation of use cases and overlays, and
- The integration of TIC 3.0 guidance in risk management programs.

The Program Guidebook articulates the following:

- An overview of the strategic goals for the TIC program,
- Guiding principles for implementing secure and flexible architectures, and
- Security objectives for securing federal networks and shared services.

3. History of TIC

Originally established in 2007, TIC initiative plays a critical role in securing the Federal Government's connections to the internet and offers vital support for the Federal Government's broader cybersecurity efforts, including, but not limited to, Cloud Smart[4], the National Cybersecurity Protection System (NCPS), and the Continuous Diagnostics and Mitigation (CDM) programs. The TIC initiative is intended to improve the Federal Government's security posture and incident response capability with a focus on strategy, architecture, and visibility.

OMB; CISA, formerly DHS's National Protection and Programs Directorate (NPPD); and GSA jointly oversee the TIC program and maintain the responsibility to keep the program modernized. These agencies continued to evolve the program to keep pace with technology; CISA's TIC guidance is now in its third iteration since the policy's establishment in 2007.

2007: TIC 1.0 – Consolidate

The TIC initiative was formally announced on November 20, 2007, with the issuance of OMB M-08-05[5]. As outlined in the initial guidance, TIC calls for the Federal Government to reduce its external network connections, including internet points of presence (POPs or access points), to 50. Through the reduction of POPs, TIC 1.0 sought to improve the Federal Government's cybersecurity posture, increase situational awareness, and improve its incident response capability.

[4] "From Cloud First to Cloud Smart," Office of Management and Budget (2019). https://cloud.cio.gov/strategy/.

[5] "Implementation of Trusted Internet Connections (TIC)," Office of Management and Budget M-08-05, (2007). https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-05.pdf.

In January 2008, the Federal Government launched the Comprehensive National Cybersecurity Initiative (CNCI) based upon NSPD 54 and HSPD 23, which included additional provisions related to the implementation of TIC capabilities. CNCI reinforced the creation of a common security solution that would allow for the eventual inspection of network traffic through these trusted points. It solidified the foundation for TIC and the NCPS EINSTEIN[6] program, which has since deployed intrusion detection sensors (IDS) across the federal enterprise to examine network traffic and identify attempts by unauthorized users to gain access to federal networks.

2011: TIC 2.0 – Standardize

Architecturally, the design between TIC 1.0 and 2.0 remained relatively unchanged. The primary difference between the two iterations of the TIC program relates to the inclusion of remote or external agency connections into the program's scope. As the TIC program evolved, DHS, in partnership with OMB, reassessed these capabilities and added new critical capabilities to improve the security of TIC. After this update, TIC had a total of 74 capabilities with over 50 considered critical. This change was incorporated into the MTIPS service to align with the latest TIC capabilities.

2019: TIC 3.0 – Modernize

Beginning in 2011, the Federal Government made strides toward migration into the cloud with the Cloud First Initiative, now known as Cloud Smart, moving its systems and data away from federally owned and operated networks. During this migration, impediments surfaced throughout implementation, including security challenges.

To better serve its citizens, the Federal Government made a concerted push to leverage technological advancements in a secure manner. As a reaction to Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*[7], the Federal Government developed a report outlining the IT modernization needs for the Federal Government. The *2017 Report to the President on Federal IT Modernization*[8] (IT Modernization Report) addresses agencies' challenges with resource prioritization, ability to procure services quickly, and technical issues by focusing on:

- Network modernization and consolidation and
- Shared services to enable future network architectures.

The IT Modernization Report calls for the modernization of TIC to improve protections, remove barriers, and enable cloud migration, marking the start of the 2019 TIC policy update. The report tasks the TIC initiative to:

- Establish TIC pilots to understand new environments,
- Update TIC policy and associated material,
- Accommodate the security needs of dispersed architectures, and
- Eliminate manual TIC Compliance Validation (TCV) Process.

[6] "EINSTEIN," Cybersecurity and Infrastructure Security Agency (2019). https://www.cisa.gov/einstein.
[7] "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Presidential Executive Order 13800 (2017). https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[8] "Report to the President on Federal IT Modernization," Office of Management and Budget (2017). https://itmodernization.cio.gov/.

To address these modernization tasks, OMB, CISA, and GSA facilitated four interagency working groups, met with several industry partners, and oversaw pilots to collect data used to inform the TIC policy update and reference architectures.

TIC 3.0 is a response to the need for improved flexibility, security, and visibility. The program is intended to be forward-leaning and environment-agnostic. TIC 3.0 broadens the concepts of the program to accommodate cloud, mobile, and encrypted applications, services, and environments. The program envisions a flexible perimeter that may protect diverse hosting environments, platforms, and services in contrast to the hard enterprise perimeter as previously implemented. While the NCPS and TIC initiatives continue to support and complement each other, the initiatives are evolving independently.

4. Strategic Program Goals

In accordance with the IT Modernization Report, CISA, in coordination with OMB, GSA, and interagency working groups, developed seven strategic goals to guide the TIC modernization effort. These goals are the guideposts for TIC 3.0, outlining the approach to securing dispersed network environments across the federal civilian enterprise to include service providers hosting federal systems and information in the cloud. These goals are reflected in all documentation.

1. Boundary-Focused

As the Federal Government continues to expand into cloud and mobile environments, systems, and assets will increasingly be dispersed which will require TIC capabilities to support diverse security services and implementation approaches. **TIC 3.0 adopts a flexible framework to address and support advanced security measures across branch offices, remote users, cloud and other service providers, mobile devices, etc.** These additional network boundaries require different placement and roles of security capabilities than those employed to protect the enterprise perimeters of federal agencies. TIC 3.0 divides agency architectures by trust zones, shifting the emphasis from a strictly physical network perimeter to the boundaries of each zone within an agency environment to ensure baseline security protections across dispersed network environments. This shift in approach from securing a single network boundary to a distributed architecture is the most fundamental change from the legacy TIC program.

2. Descriptive, Not Prescriptive

The past iterations of the program focused on securing traffic at the physical agency network perimeter through a limited number of secured access points that had a required set of security appliances and services. With advances in technology, the federal IT landscape has shifted markedly since the TIC program's initiation in 2007, rendering this one-size-fits-all approach inflexible and counterproductive to meet the demands to modernize and move to the cloud. The updated reference architecture, taxonomy, capabilities, and use cases will broaden the concepts of the program to accommodate cloud, mobile, and encrypted applications, services, and environments. These documents will provide guidance to agencies to implement the TIC initiative in a manner that best suits their needs.

3. Risk-Based to Accommodate Varying Risk Tolerances

Federal agencies have varying degrees of risk tolerances that must be considered as IT modernization tasks are planned and executed. Agencies must determine the level of controls and consider the security capabilities that are necessary to secure their environments. In some cases, the controls identified in the TIC 3.0 documentation may not provide enough security to adequately address residual risks necessary to protect information and systems. In cases where additional controls are necessary to manage residual risk, agencies are obligated to apply the controls or explore options for compensating controls that achieve the same protections to manage risks. TIC 3.0 encourages vendors and agencies to develop and maintain TIC overlays to assist agencies with identifying products and services that can be applied to secure their environments. To the extent practical, agencies are encouraged to leverage existing enterprise capabilities

capable of providing protections for on-premise or service provider hosting environments, to include those provided by the CDM program.

4. Environment-Agnostic

Every agency operates with unique missions, business needs, resource availability, and risk tolerances. To maximize the applicability of TIC guidance, the terms, definitions, and logical components of network infrastructure and solutions are vendor and technology-neutral. Additionally, the modernized TIC guidance provides flexibility on the application of the security capabilities to accommodate a variety of agency environments; these are captured in the TIC use cases.

5. Dynamic and Readily Adaptable

To keep pace with technological innovation, CISA will continue to produce and update use cases and overlay guidance through collaboration with agencies and vendors to maintain relevancy. CISA will also update core guidance, reference architectures, and capabilities based on agency and public feedback, evolving threats, and emerging cybersecurity trends.

6. Automated and Streamlined Verification

In accordance with the IT Modernization Report, the modernized TIC initiative eliminates the existing TIC-related FISMA metrics and manual TIC Compliance Validation (TCV) process with the intent to replace both with an automated metric collection as applicable. The primary focus of the validation is security and availability measures. The validation will leverage existing capabilities under the CDM and NCPS program. The program's goal is to define scalable, comprehensive, and continuous validation processes for ensuring agency implementation of TIC capabilities in contrast to the point-in-time reviews.

7. Delineate the NCPS and TIC Initiatives

CISA continues to provide the security capabilities in accordance with the Federal Cybersecurity Enhancement Act of 2016[9] to protect "all information traveling between an agency information system and any information system other than an agency information system." The NCPS EINSTEIN and TIC initiatives will continue to support and complement each other in support of this legislation. However, CISA will provide independent guidance for each of the respective programs. Additional information regarding the relationship between the TIC and NCPS initiatives can be found in Section 14.

5. Security Objectives of TIC 3.0

As the Federal Government continues to expand into cloud and mobile environments, an agency's assets, data, and components are commonly located in areas beyond their network boundary – on remote devices, at cloud data centers, with external partners, etc. To protect these dispersed assets, the TIC program defines encompassing security objectives to guide agencies in securing their network traffic. The objectives intend to limit the likelihood of a cybersecurity event. Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected.

Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected.

[9] Federal Cybersecurity Enhancement Act of 2016, S. 1869 (2016). https://www.congress.gov/bill/114th-congress/senate-bill/1869/text.

The TIC security objectives should be viewed independently of the types of traffic being secured, but different types of traffic will influence how the objectives are interpreted. Each objective stands on its own, independent of the other objectives. They should not be considered an order-of-operations. In other words, the intent of the objectives is not to suggest that an agency must execute one objective to execute another.

The TIC objectives, described in Table 3, are intended to set expectations for architectures, guide implementation, and establish clear goals at the network level. The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones or stored at either or both trust zones.

Table 3: TIC 3.0 Security Objectives

Objective[10]	Description
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures

[10] The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones or stored at either or both trust zones.

The TIC security objectives can be mapped to the five functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[11]: Identify, Protect, Detect, Respond, and Recover. The relationship between the CSF and TIC security objectives is depicted in Figure 2. Furthermore, the TIC security capabilities are mapped to the NIST CSF in the TIC 3.0 Security Capabilities Catalog (Security Capabilities Catalog). This mapping will facilitate the development of TIC overlays for several of the more widely used vendors.

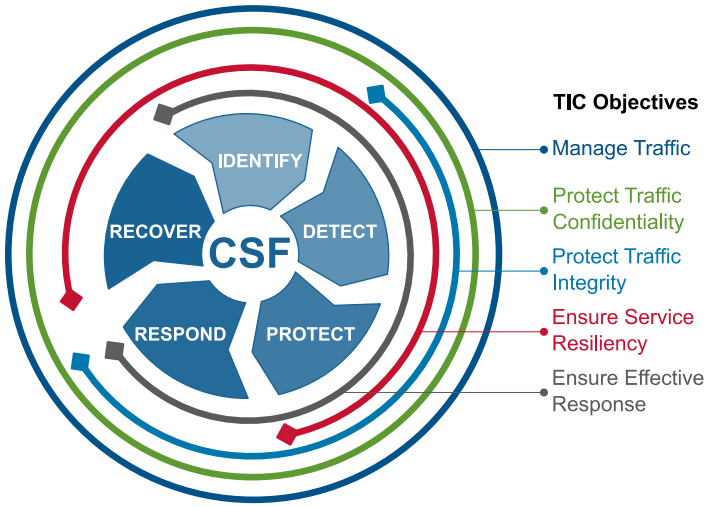

Figure 2: TIC Lens on the Cybersecurity Framework Functions

6. Modernization Transition Strategy

The TIC modernization effort is a response to the technological advances made in recent years within the information technology space and specifically cloud, mobile, and encryption technology. To allow flexibility for federal agencies to incorporate new technology concepts in modernizing their network infrastructure, the existing TIC architecture adopts a flexible framework and capabilities to keep pace with increasing demand.

CISA advocates applying the NIST CSF functions towards the intent of TIC. The aim is to provide agencies with a broad range of options to choose from when considering infrastructure projects. In short, the TIC modernization effort:

- Accommodates modern computing architectures,
- Promotes cloud adoption,
- Provides agencies the flexibility to implement secure capabilities that are consistent with their missions and risk tolerance, and
- Incorporates new technologies through frequent updates to TIC documentation.

[11] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology SP 800-53 Rev 1.1 (2018). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

The modernized program advocates for smaller segmentation of an agency's environment to enforce security capabilities and controls closer to the data, applications, and systems they are protecting.

The modernized program advocates for smaller segmentation of an agency's environment to enforce security capabilities and controls closer to the data, applications, and systems they are protecting.

The modernized program advocates for smaller segmentation of an agency's environment to enforce security capabilities and controls closer to the data, applications, and systems they are protecting. Figure 3 shows how the deployment of TIC security capabilities changes in TIC 3.0. TIC security capabilities are dispersed across the environment on multiple policy enforcement points (PEPs) rather than exclusively at the TIC access point, as in TIC 2.0. The PEPs consist of focused security capabilities based on the environment or location they are implemented.

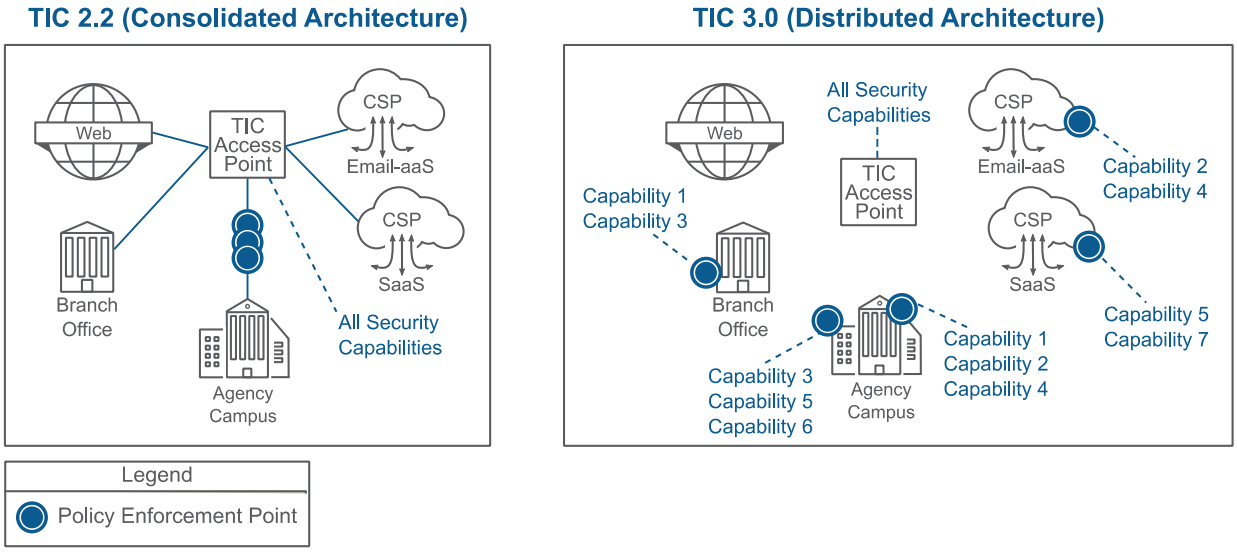

Figure 3: Transition from a Consolidated to Distributed Security Architecture

6.1 Core Program Updates

Several core updates are present in the TIC 3.0 guidance that were distilled in collaboration with agency stakeholders, through several interagency working groups, industry participation, and pilots. The updates introduce new concepts, capabilities, and approaches that established a foundation for TIC 3.0. The following is a summary of the core updates:

- **Introduction of Trust Zones:** Past TIC documentation presented strictly-defined approaches to trust; new TIC documents eschew this "one-size-fits-all" approach in favor of a more nuanced view that recognizes the reality that the definition of "trust" may vary across federal agencies and specific computing contexts. The TIC 3.0 guidance introduces trust zones as a tool for agencies to tailor the security capabilities to their risk tolerance.
- **Update to the Security Capabilities:** The Security Capabilities Catalog features additions, deletions, and modifications of capabilities to reflect a decade's worth of technological evolution, policy and program developments, and stakeholder feedback. Agencies have significant discretion regarding how to meet the individual security capabilities. Guidance for the application of TIC security capabilities will be given within TIC use cases.

- **Adoption of Risk-Based Approach:** The Security Capabilities Catalog discards the "Critical/Recommended" capability prioritization approach utilized in previous versions. In TIC 3.0, agencies are encouraged to implement TIC use cases using a risk management approach.
- **Adoption of Multiple Policy Enforcement Points:** TIC use cases support multiple security approaches that focus on protecting agency data transmitted and protecting data stored beyond agency network boundaries. The use cases demonstrate scenarios that accommodate a distributed deployment of TIC capabilities across multiple PEPs, in addition to, or instead of, deployment of a single TIC PEP implementation for external connections.
- **Introduction of TIC Use Cases:** Instead of defining TIC security patterns based on connection classes (e.g., external, internal), TIC 3.0 introduces TIC use cases. The purpose of each TIC use case is to identify the applicable security architectures, data flows, and PEPs and describe the implementation of security capabilities in a given scenario. TIC use cases will also identify data flows where telemetry must be sent to CISA.
- **Restructure of Documentation Set:** Previously, a reference architecture functioned as the primary source of TIC guidance. In TIC 3.0, guidance is presented as a set of documents, which includes this guidebook, a reference architecture, a catalog of security capabilities, individual use cases, and guidance for how vendors and agencies can develop overlays. This approach allows for more agile modifications of all TIC-related guidance (e.g., changes to individual capabilities will no longer require re-approval of the full set of guidance).
- **Introduction of TIC Overlays:** The modernized guidance introduces overlays as a tool for agencies to leverage when implementing the TIC guidance. The *TIC 3.0 Overlay Handbook* (Overlay Handbook) provides guidance for how vendors and agencies can create an overlay that maps products and services to TIC security capabilities. Agencies can use these overlays to make decisions on how to deploy TIC security capabilities as they implement TIC use cases.
- **Alignment of Terminology and Concepts:** TIC 3.0 deprecates some of the terms previously utilized by the TIC program and aligns the TIC initiative with current industry and government best practices.

7. Key Program Documents

TIC 3.0 documents, listed in Figure 4, are intended to be used collectively in order to achieve the goals of the program. The documents are additive; each builds on the other like chapters in a book. The set of TIC documents is depicted in Figure 4 and described in detail below.

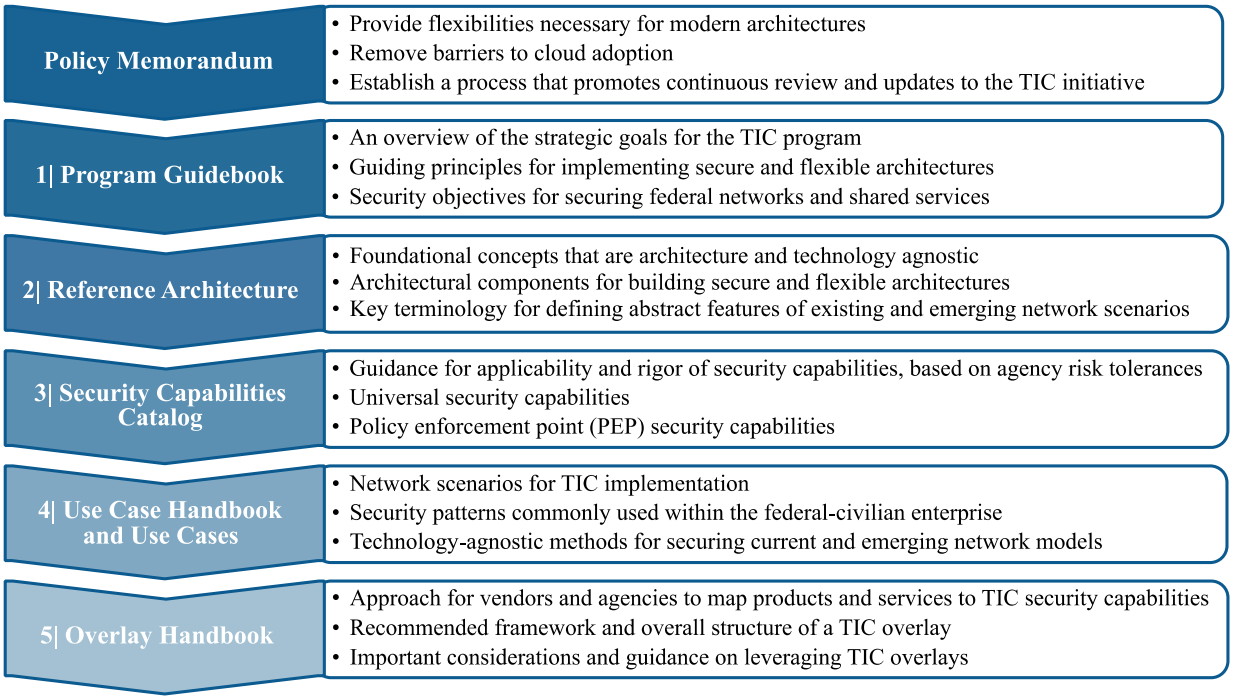

Figure 4: TIC 3.0 Key Program Documents List

Policy Memorandum

Beginning with the TIC policy memorandum, OMB M-19-26 lays the foundation for the program. It outlines the OMB expectations for TIC to provide flexibilities necessary for modern architectures, remove barriers to cloud adoption, and establish a process that promotes continuous review and updates to the TIC initiative. CISA is responsible for articulating the expectations outlined in the memorandum through the subsequent documents.

Volume 1: Program Guidebook

The Program Guidebook begins to articulate CISA's translation of the OMB M-19-26 into concrete TIC guidance. The guidebook describes core modifications to the TIC program, provides historical context of the TIC program, and illustrates how agencies can implement TIC 3.0 as they adopt modern architectures. The Program Guidebook also clarifies the relationship that TIC has to other initiatives, programs, and entities in the Federal Government, such as the NIST CSF, FedRAMP, and the NCPS program.

Volume 2: Reference Architecture

The Reference Architecture builds on the Program Guidebook, detailing the key concepts of the program to guide and constrain the instantiations of the TIC use cases. The Reference Architecture describes the baseline implementation of TIC 3.0, in which all agency traffic flows through a physical TIC access point. The Reference Architecture also describes how PEPs and security capabilities must be in place for scenarios in which traffic may not flow through a physical TIC access point.

Volume 3: Security Capabilities Catalog

Complementary to the Reference Architecture, the Security Capabilities Catalog features an index of security capabilities applicable to the TIC security objectives. The TIC security capabilities include universal security capabilities, which are applicable at the enterprise level, and PEP security capabilities that can be applied at several PEPs. TIC security capabilities are mapped to the NIST Cybersecurity Framework. Guidance for implementing security capabilities will be provided in TIC use cases.

Volume 4: TIC Use Case Handbook and Use Cases

The Reference Architecture and the Security Capabilities Catalog create the foundation for the TIC use cases. The use cases provide examples of architectures and provide guidance on the secure implementation and application of security capabilities to applications, services, and environments. TIC use cases give cybersecurity guidance to accommodate the use of cloud, mobile, and other computing environments in the Federal Government.

Volume 5: Overlay Handbook

The Overlay Handbook gives guidance on how vendors and agencies can develop TIC overlays. Agencies can use the resulting overlays to assess the capabilities of the vendors, to make decisions on the procurement of products and services, and to identify any potential security capability gaps that need to be addressed.

All key documents will be refreshed as changes occur in the technological landscape, emerging cybersecurity threats, and strategic priorities. Feedback from agencies and industry will also be considered.

8. Security Capabilities, Use Cases, and Overlays

Since 2017, CISA has been involved in technical discussions with agencies and vendors to explore capabilities and service offerings, focusing on the cloud, that can be applied to support TIC objectives and capabilities. Key observations indicate the following:

- Agencies may have investments in enterprise network and security tools that can be utilized to support TIC capabilities for cloud implementations.
- Vendors have significant capabilities that implement the TIC capabilities. Agency architecture or operating needs, customization, and/or additional third-party capabilities may need to be applied to address gaps.
- Vendor capabilities are in a constant state of development to enhance their offerings.
- TIC overlays may apply to multiple use cases.

Based on these key observations, CISA identified a need to decouple the TIC security capabilities from the use cases to support efficient lifecycle management and to permit vendors to self-describe how their services can be leveraged. The three independent work products are:

First, the **TIC Security Capabilities Catalog** provides an index of security capabilities that are used to meet TIC security objectives. The capabilities captured will evolve with ecosystem innovations, independent of the TIC use case and TIC overlay update cycle.

Second, **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 PEPs and to describe the implementation of the security capabilities in a given scenario.

The use cases include details on:

- Security patterns,
- Implementation of TIC security capabilities, and
- CISA telemetry guidance.

Third, **TIC overlays** contain mappings from TIC security capabilities to products and services, independent of TIC use cases. Vendors and agencies are encouraged to develop TIC overlays using the Overlay Handbook. CISA recommends agencies and vendors continuously review and update their overlays to keep pace with their new products and services.

9. TIC Pilot Process

A key feature of the TIC policy update includes the ability for agencies to conduct TIC pilots to leverage modern architectures and technology to improve an agency's IT infrastructure and cybersecurity posture. A TIC pilot is a representation of an agency architecture that assesses the feasibility and utility of the modern architecture under the TIC guidance. TIC pilots reveal insights into different ways of meeting TIC objectives and implementing TIC security capabilities. Results and lessons learned from the TIC pilots will inform TIC use cases.

The *TIC 3.0 Pilot Process Handbook*[12] should be used by agencies and vendors to find more details on the following:

- The relationship between TIC pilots and TIC use cases,
- The process agencies and vendors can use to propose TIC pilots,
- The process used to execute TIC pilots and develop TIC use cases, and
- The roles and responsibilities of key stakeholders in the TIC pilot process.

10. Integrating TIC into a Risk Management Plan

In accordance with OMB M-19-26, legacy TIC policy deprecation facilitates flexibility to employ TIC capabilities to remove barriers to adopting modern technologies. The legacy TIC policies relied on DHS TIC Compliance Validation (TCV) assessments that served as a compliance mechanism to account for required TIC capabilities employed at an agency TIC or TICAP.

The flexibilities afforded in OMB M-19-26 shifts responsibility for compliance with TIC capabilities to the agency. **This provision is intended to allow agencies to examine TIC security capabilities in the context of the TIC guidance that meet their business and risk management needs.** Agencies will need to carefully consider and evaluate technologies and implementation approaches offered by system integrators or vendors to ensure that risk can be managed in accordance with thresholds set by the agency.

[12] "Trusted Internet Connections 3.0 Pilot Process Handbook," Cybersecurity and Infrastructure Security Agency, December 2019 (Draft). https://www.cisa.gov/trusted-internet-connections.

As shown in Figure 5, TIC use cases provide architecture solutions, the Security Capabilities Catalog gives an index of cybersecurity protections, and TIC overlays provide potential solutions for use cases. Agencies can use these TIC documents, along with the NIST CSF and NIST SP 800 53, and any other cybersecurity requirements documents. Using this collection of TIC documents, along with NIST CSF and NIST SP 800-53, agencies can implement TIC into their dispersed environment while meeting all necessary telemetry requirements. In accordance with OMB M-19-26, agencies maintain responsibility for implementing the use cases and employing applicable overlays to ensure their environment is secure.

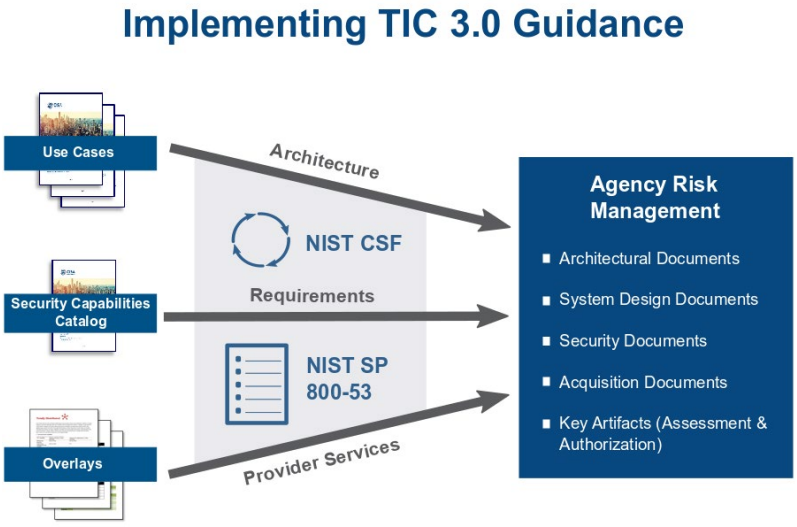

Figure 5: How an Agency Can Integrate TIC into an Agency Risk Management Plan

Due to the wide variety of modern IT environments and requirements based upon the agency's missions, needs, and resources, the updated policy allows for broader interpretation authorities to be assumed by the agencies. As modern architectures become both more complex and diverse, TIC 3.0 accommodates a wide variety of scenarios, focusing on cloud, mobility, and encryption. TIC 3.0 guidance intentionally has a different tone and level of detail when compared to earlier iterations to accommodate this wider variety of environments. The guidance is meant to be abstract, conceptual, high-level, notional, and theoretical to convey the intention of the concept while allowing agencies the flexibility they require to interpret the guidance as best fit their needs. Telemetry can be used to identify unexpected or improper data activity of agency users or unidentified internal users.

The guidance is meant to be abstract, conceptual, high-level, notional, and theoretical to convey the intention of the concept while allowing agencies the flexibility they require to interpret the guidance as best fit their needs.

Vendors offer technologies that fully or partially meet the TIC capabilities. In order to support agency risk management responsibilities, agencies should follow the FedRAMP process and determine if the vendor is authorized[13]. In the event the vendor is not FedRAMP authorized or in the process of obtaining authorization, agencies are responsible for assessment and authorization. CISA continues to closely collaborate with the FedRAMP PMO.

[13]"FedRAMP Marketplace," General Services Administration, https://marketplace.fedramp.gov/#!/products?sort=productName.

11. Telemetry Requirements

The Federal Information Security Modernization Act of 2014 (FISMA)[14] codifies DHS's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies. As such and in accordance with NSPD-54 and HSPD-23, TIC requires agencies to comply with all applicable telemetry requirements.

The implementations of security capabilities produce artifacts that provide visibility into the agency's environment and security posture. However, the Security Capabilities Catalog does not detail the telemetry that agencies need to provide to CISA programs such as NCPS and CDM. Since visibility needs will often align, this telemetry may be used for both CISA and agency purposes. Agencies remain free to address any unique telemetry requirements beyond those from CISA. As agencies implement solutions and adopt use case recommendations, they can generate mappings of their solutions to TIC security capabilities to ensure coverage. When applicable, TIC requires agencies to provide self-attestation on their adherence to the program guidance.

TIC telemetry does not replace or negate the telemetry required by other CISA programs, including NCPS and CDM. Agencies should align the telemetry collection, processing, and sharing needs to ensure full compliance.

11.1 TIC Information Cycle

As CISA programs evolve to accommodate new service delivery models and multi-boundary protections, they establish an information lifecycle with agencies and other entities, as illustrated in Figure 6. The TIC information lifecycle is as follows.

1. CISA provides guidance on strategy, architecture, and visibility to agencies.
2. Agencies review CISA guidance and TIC overlays with consideration for their risk tolerances when selecting and configuring services.
3. Agencies provide telemetry of their operating environments to CISA.
4. Trust zones deliver services, as configured, and provide agencies visibility.

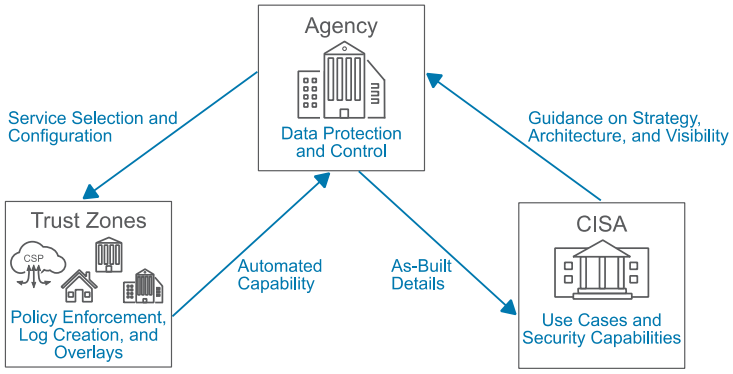

Figure 6: TIC Information Cycle

[14] "Federal Information Security Modernization Act," Cybersecurity and Infrastructure Security Agency, April 2020. https://www.cisa.gov/federal-information-security-modernization-act

12. Agency Engagement

Each agency is a stakeholder in the TIC initiative and its input is critical to the overall success of the program. CISA traditionally engages with the agency CIOs, CISOs, and designated technical subject matter experts (SMEs), known as TIC delegates, to ensure that each agency has a voice and opportunity to contribute to the program. References to CIO and CISO are directed at the department/headquarters CIO and CISO. Agency TIC Delegates serve an important role to support CISA. The role of the TIC Delegate is to be:

- Familiar with the agency's network architecture and security solutions including TIC, email, security and cloud architecture(s);
- Able to contribute to TIC Working Group meetings;
- Able to represent the agency, and coordinate views of all offices such as CIO, CISO, Risk, CTO, and Information Assurance;
- Able to be the liaison between the agency CIO Office, the agency programs interested in the TIC initiative, and CISA's CISA; and
- Able to express how the agency wants the TIC initiative to support its activities.

13. TIC Service Options

OMB M-19-26 deprecated the original policies that categorized agencies as TICAPs and Seeking Service Agencies. However, for the *TIC 3.0 Traditional TIC Use Case* (Traditional TIC Use Case), agencies can maintain existing TIC compliance and relationships under the legacy policy construct but may leverage the flexibilities in the policy update for other use cases. Hence, agencies will align with at least one of the following options when implementing the Traditional TIC Use Case, as per the policy update.

TIC Access Providers

The TIC Access Provider, or TICAP, is an agency that owns and operates a TIC access point that is secured by a network operations center (NOC) and security operations center (SOC). The TIC access points can be managed by the agency or a service provider that specializes in providing security services. The risk tolerance and performance needs of the agency's information system infrastructure and network would drive how the TICAP should be architected.

Seeking Services Agencies and MTIPS

Agencies that do not manage their own TIC access points are considered Seeking Service Agencies (SSA). SSAs must work through a Multi-Service TICAP or Managed Trusted Internet Protocol Services (MTIPS) to obtain TIC services. MTIPS are managed services provided under the EIS contract vehicles, managed by GSA, that can be acquired by an agency that does not manage their own TIC access point. An MTIPS offers specialized managed security services as an alternative to using existing TICAPs.

EIS also accommodates a model that reflects that of a managed security service (MSS), where agencies select the specific MTIPS capabilities that they require rather than the entire package of MTIPS services.

14. TIC and Other Initiatives

TIC 3.0 complements other federal initiatives that are focused on issues like cloud adoption and federal enterprise network security. This section details the relationship between TIC and other federal initiatives and programs.

TIC and Federal Risk and Authorization Management Program

The Federal Risk and Authorization Management Program (FedRAMP)[15] is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Ensuring that TIC and FedRAMP work together is key to securing remote networks. CISA coordinates regularly with the FedRAMP PMO.

TIC and National Institute of Standards and Technology Zero Trust Architecture

The NIST Zero Trust Architecture (ZTA) principles in SP 800-207 (Draft)[16] assume all networks are hostile and promote the continuous evaluation of access to network resources to maintain security. ZTA guidance can be used to secure cloud-based resources, as well as remote user access to assets on or off-premises. ZTA concepts support instantiations of TIC 3.0 architectures; the trust of a zone is designated independently of adjacent zones, and an agency can designate all trust zones as having low trust. Security capabilities from adjacent trust zones and traffic between zones must be continuously evaluated.

TIC and CIOC Cloud Smart

The CIOC Smart Cloud strategy supports the accelerated adoption of cloud-based solutions at federal agencies.[17] The strategy is based on three pillars (security, procurement, and workforce) required for successful cloud adoption and provides agencies with recommendations and implementation guidance based on public and private sector use cases. TIC supports the Cloud Smart initiative by supplying agencies with use cases and overlays to reference when selecting cloud-based security capabilities.

TIC and GSA Enterprise Infrastructure Solutions

The GSA EIS contract vehicle enables the Federal Government to acquire more technologically current telecommunications and IT infrastructure solutions.[18] EIS allows agencies to procure emerging technologies as they become commercially available and is expected to provide agencies with industry suppliers who deliver complete portfolios of cybersecurity solutions. The EIS Managed Trust Internet Protocol Service (MTIPS) protects agencies' logical and physical connections to external connections and the internet. MTIPS supports TIC goals such as the reduction and consolidation of external access points across the federal enterprise.

TIC and Continuous Diagnostics and Mitigation

Fully aligned with the Federal Government's deployment of Information Security Continuous Monitoring (ISCM), the CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems.[19] The CDM program provides cybersecurity tools, integration services, and dashboards to participating agencies to support them in improving their respective security posture. CDM aligns with TIC 3.0 capabilities by providing visibility into an agency network(s) particularly through the Network Security Management (NSM) capability area. However, as networks mature and modernize, other CDM

[15] "FedRAMP", https://www.fedramp.gov/.

[16] "Zero Trust Architecture (NIST SP 800-207)," 2nd Draft, February 2020. https://csrc.nist.gov/publications/detail/sp/800-207/draft.

[17] "Federal Cloud Computing Strategy", https://cloud.cio.gov/.

[18] "U.S. General Services Administration Enterprise Infrastrcture Solutions", https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-infrastructure-solutions.

[19] "Continuous Diagnostics and Mitigation (CMD)", https://www.cisa.gov/cdm.

capability areas such as Identity and Access Management (IDAM) will provide visibility to key access management information; all of which will support TIC concepts such as trust zones and PEPs.

TIC and High Value Assets

High Value Assets (HVA)[20] are assets where the information or information system processes, stores, or transmits information of high value to the Federal Government or its adversaries, the information or information system performs a primary mission essential function (PMEF) for the agency, or the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise. TIC 3.0 supports agencies that operate with "a strategic enterprise-wide view of risk" to identify trust zones that contain HVAs and to apply rigorous security capabilities accordingly, consistent with OMB M-19-03: *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*[21].

TIC and National Cybersecurity Protection System

As agencies move their information technology infrastructure to the cloud, some of their network traffic no longer traverses traditional NCPS sensors, and security information about that traffic may no longer be captured by NCPS. The NCPS program is evolving to ensure that security information about cloud-based traffic can be captured and analyzed and CISA analysts can continue to provide situational awareness and support to the agencies. To support this goal, CISA is deploying a cloud-based architecture, the Cloud Log Aggregation Warehouse (CLAW), to collect and analyze agency cloud security data. The *NCPS Cloud Interface Reference Architecture* (*NCIRA*)[22], which is being released in two volumes, explains how agencies can provide cloud-generated security information to that system. Agencies can refer to the NCIRA for guidance on telemetry. Additional information about NCPS authorities can be found in Appendix A.

15. Conclusion

In early iterations, the TIC initiative's main goal was to consolidate TIC access points and develop a federal perimeter security baseline to secure the federal network landscape. The TIC 3.0 program expands on the existing foundation by adding new concepts that allow for increased flexibility to federal agencies in their quest for hardening network security or acquiring new technologies. The Program Guidebook provides an overview of the TIC program artifacts including the OMB M-19-26, the Reference Architecture, Security Capabilities Catalog, and the TIC use cases. Upon completion of this guidebook, agencies should understand the history of the program, the modernization effort, and the expectation of TIC 3.0.

[20] "Federal High Value Asset Program Management Office (HVA PMO)", https://www.cisa.gov/hva-pmo.

[21] "*Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*," Office of Management and Budget M-19-03 (2018). https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf.

[22] National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture: Volume 1 General Gudiance and Volume 2 Reporting Pattern Catalog, to be released 2020.

Appendix A – TIC and NCPS Program Authorities

The TIC and NCPS initiatives are further described in the established by Joint Presidential Directive NSPD-54/HSPD-23; OMB M-19-26, Update to the Trusted Internet Connections (TIC) Initiative. These documents provide further details on agency, OMB, and DHS responsibilities and reporting requirements, acquisition vehicles, and technical capabilities under the TIC initiative. The Homeland Security Act, as amended by section 223 of the Federal Cybersecurity Enhancement Act of 2015, Consolidated Appropriations Act of 2016 (Pub. L. No. 114-113, 129 Stat. 2242, Division N, Title II, Subtitle B), requires DHS to "deploy, operate, and maintain" and "make available for use by any agency" capabilities to detect cybersecurity risks in agency network traffic and take actions to mitigate those risks (6 U.S.C. § 663(b)(1)). DHS currently provides these capabilities through its NCPS program and, as required by law, ensures all retention, use, and disclosure of information obtained through NCPS occurs only for protecting information and information systems from cybersecurity risks (See id. § 663(c)(3)). The Federal Cybersecurity Enhancement Act of 2015 also requires agencies to apply these capabilities to "all information traveling between an agency information system and any information system other than an agency information system." Id. § 663, note.

Appendix B – Key Federal Policy and Directives

LEGISLATION

Federal Information Security Modernization Act (P.L. 113-283), December 2014.

KEY POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

National Security Presidential Directive (NSPD) 54, Cyber Security and Monitoring, 8 January 2008. Also known as HSPD-23.

Homeland Security Presidential Directive (HSPD) 23, Computer Network Monitoring and Cyber-security, 8 January 2008. Also known as NSPD-54.

Office of Management and Budget (OMB) Memorandum M-19-26: Update to the Trusted Internet Connections (TIC) Initiative, 12 September 2019.

GUIDELINES

National Institute of Standards and Technology Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018.

National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Appendix C – 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 close out by 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.