Trusted Internet Connections 3.0

Vol. 1:

Program Guidebook

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Document Status

This document is a draft and open for public comment. The Cybersecurity and Infrastructure Security Agency is requesting feedback and comments through January 31, 2020.

Acknowledgements

This modernization effort is the product of ongoing multi-agency collaboration to provide additional guidance for the successful implementation of the Trusted Internet Connections (TIC) initiative. Several agencies provided resources to support the modernization effort of the TIC initiative.

Key Stakeholders

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)
- General Services Administration (GSA) Enterprise Infrastructure Services (EIS)
- General Services Administration (GSA) Federal Acquisitions Service (FAS) Office of Information Technology Category (ITC)
- Federal Chief Information Officers Council (CIOC)
- Federal Chief Information Security Officers Council (CISOC)
- Federal Small Agency Chief Information Officers Council (SACC)
- Office of the Federal Chief Information Officer (OFCIO)
- Office of the Federal Chief Information Security Officer (OFCISO)
- National Institute of Standards and Technology (NIST)

Strategic Contributors

- 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
- Ashley Mahan, General Services Administration
- Rob McKinney, Environmental Protection Agency
- Eric Mill, Individual
- Stu Mitchell, Industry
- Brian Moore, Department of State
- Sara Mosley, Federal Deposit and Insurance Corporation
- Stuart Ott, Department of the Interior
- Travis Richardson, Department of Health and Human Services
- Maria Roat, Small Business Administration
- 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 1: 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.

Since 2007, 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 TICs 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 IT Modernization* identified TIC 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 IT and cybersecurity approaches to protect assets. Results and lessons learned from the TIC pilots will inform the TIC Use Cases, developed to support 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 is derived from the NSPD 54 and HSPD 23. The following OMB Memoranda 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:

- OMB Memorandum M-19-26: *Update to the Trusted Internet Connections (TIC) Initiative*

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 Documentation

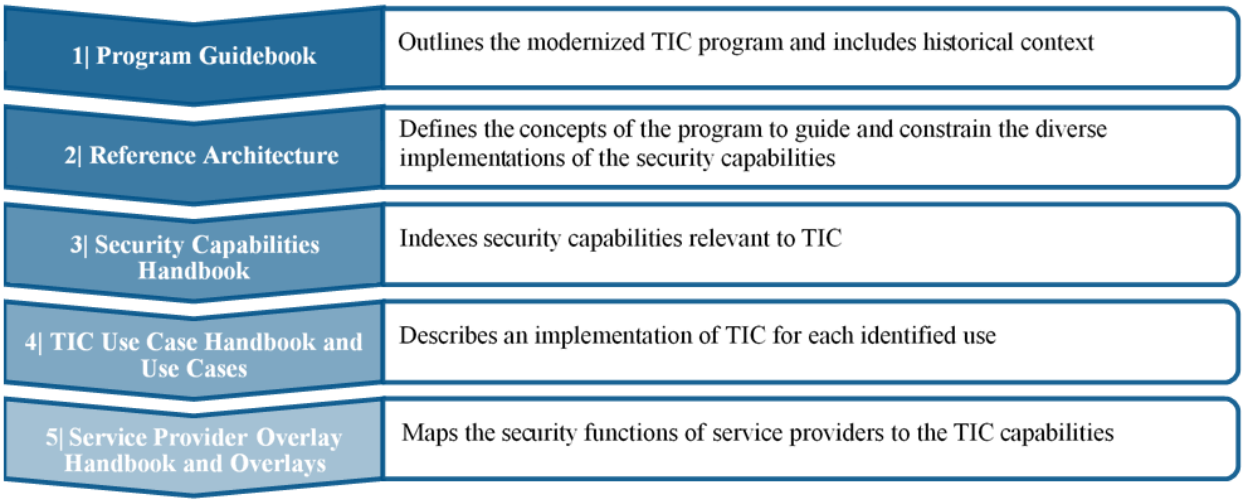
The scope of the TIC 3.0 documentation encompasses the TIC initiative and other federal program artifacts and publications necessary to explain key elements, goals, and objectives of TIC 3.0. Publications and artifacts may consist of acquisition, technical, and non-technical procedures and policies that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

The primary audience of the TIC 3.0 documentation includes federal civilian agencies, contractors, and vendors that are required to comply 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 initiative is defined through key documents that describe the directive, the program, the capabilities, the implementation guidance, and a mapping to service providers. Each document has an essential role in describing TIC and its implementation. The documents provide an understanding of how changes have led up to the latest version of TIC and why those changes have occurred. The documents go into high-level technical detail to describe the exact changes in architecture for TIC 3.0. The documents are additive; each builds on the other like chapters in a book. As depicted in Figure 1, the documents should be referenced in order and to completion to gain a full understanding of the modernized initiative.

Figure 1: TIC 3.0 Implementation Reader's Guide



TIC 3.0 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 perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative, setting requirements and an execution framework for agencies to implement a baseline perimeter security standard.

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

1.1 Key Terms

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

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

Hybrid TIC Model: An alternative approach to implementing TIC services that blends the use of agency hosted and managed TIC access providers (TICAP) and MTIPS solutions.

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

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

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

Management Entity (MGMT): A notional concept of an entity that oversees and controls the protections for data. The entity can be an organization, network device, tool, function or application. The entity can control the collection, processing, analysis, and display of information collected from the 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: Used to articulate security best practices and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means (i.e., functionality in hardware,

[1] “Update to the Trusted Internet Connections (TIC) Initiative,” Office of Management and Budget M-19-26 (2019). < https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf >.

software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

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

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

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

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

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

2. Purpose of the Program Guidebook

The 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,
- Direction for the program outlined in the IT Modernization Report,
- Core updates and changes to the program,
- TIC 3.0 documents and how to use them,
- Use of TICAPs and MTIPS in the modernization program,
- High-level implementation of Use Cases and Overlays, and
- Integration of TIC 3.0 in risk management programs.

3. History of TIC

Originally established in 2007, TIC 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[2], 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, through the reduction and consolidation of external connections and the implementation of baseline security standards.

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

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

2007: TIC 1.0 – Consolidate

The TIC initiative was formally announced on November 20, 2007, with the issuance of OMB Memorandum M-08-05[3]. 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.

In January 2008, President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI) based upon NSPD 54 and HSPD 23 (NSPD-54/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[4] 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 51 considered critical. This change was incorporated into the MTIPS contract 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*[5], OMB, DHS, and GSA developed a report outlining the information technology (IT) modernization needs for the Federal Government. The *2017 Report to the President on Federal IT Modernization (IT Modernization Report)*[6] addresses agencies' challenges with resource prioritization, ability to procure services quickly, and technical issues by focusing on:

- Network Modernization and Consolidation
- Shared Services to Enable Future Network Architectures

[3] "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.

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

[5] "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/.

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

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.

To address these modernization tasks, OMB, CISA, and GSA facilitated four interagency working groups 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 and GSA, 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 and requirements associated with the program.

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. 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 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 TIC 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 consider the security capabilities that are necessary to secure TIC 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 leverages cloud and other service providers to develop and maintain security control overlays to assist agencies with identifying service provider capabilities 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.

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 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, the TIC Program Management Office (PMO) will continue to produce and update use cases and overlays through collaboration with agencies and service providers to maintain currency. The TIC PMO 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, replacing both with 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 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 2015* 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. The NCPS PMO and TIC PMO will independently provide guidance for their respective initiatives. Additional information regarding the relationship between the TIC and NCPS initiatives can be found in Appendix A.

5. Modernization Transition Strategy

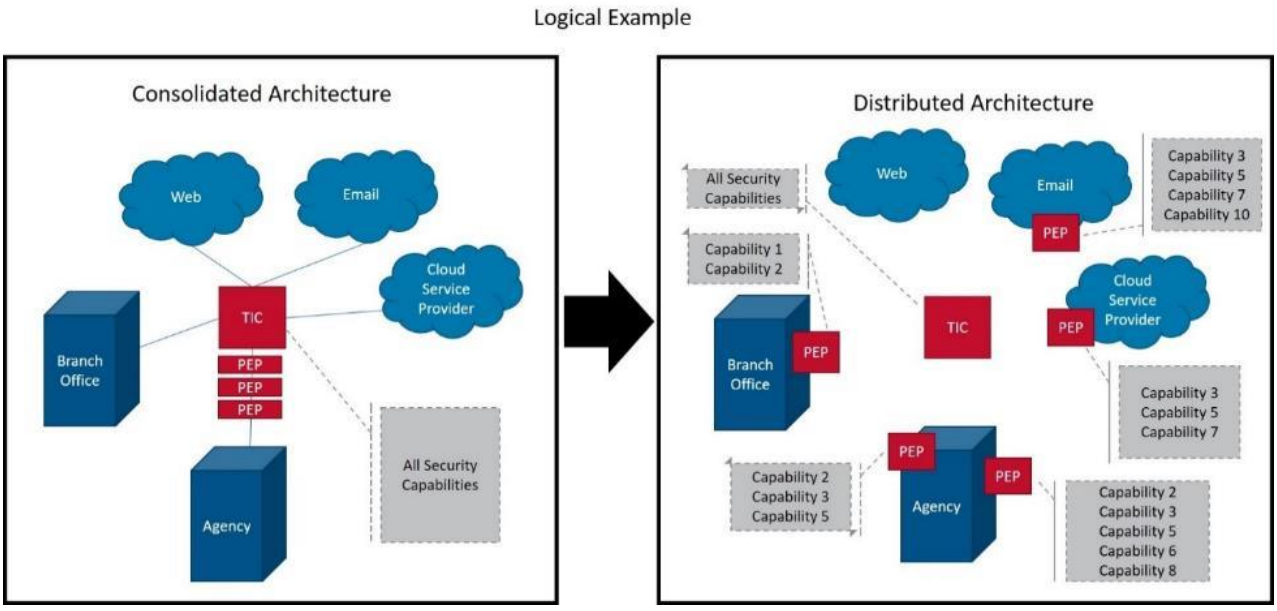
The TIC modernization effort is a response to the technological advances made in recent years within the information technology space and specifically cloud, mobile, and encryption technology. To allow flexibility for federal agencies to incorporate new technology concepts in modernizing their network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

The TIC PMO advocates applying the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) functions—Identify, Protect, Detect, Respond, and Recover—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.

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. Unlike TIC 2.0, the security capabilities are dispersed across the environment on PEPs rather than exclusively at the TIC Access Point. The PEPs consist of focused security capabilities based on the environment or location they are implemented.

Figure 2: Transition from a Consolidated to Distributed Security Architecture



5.1 Core Program Updates

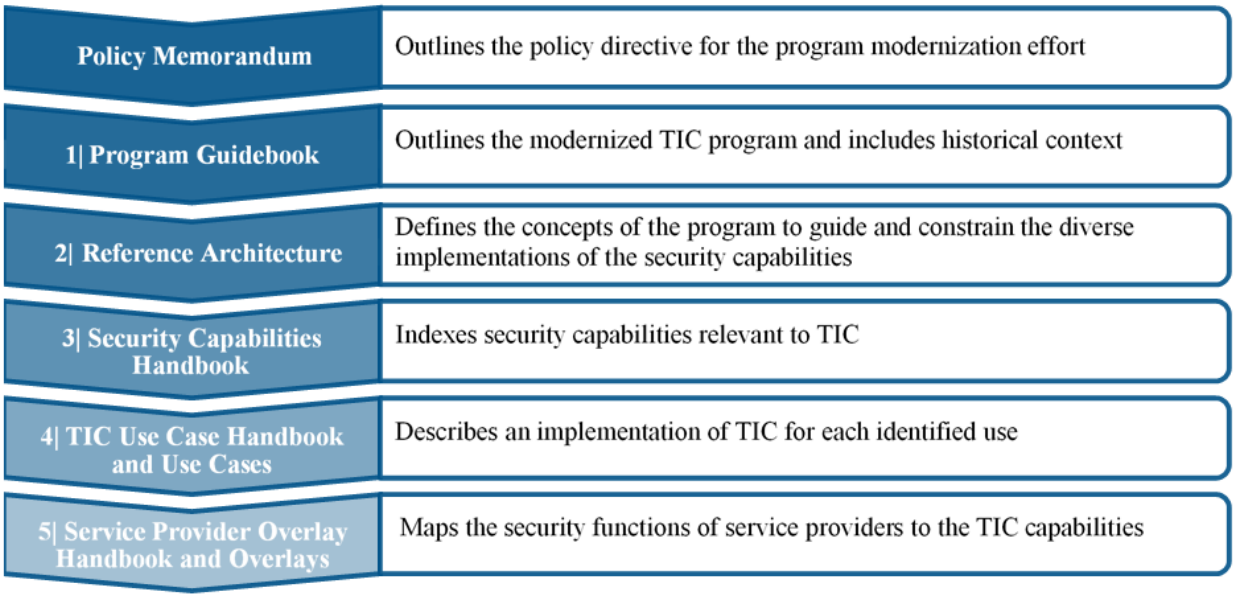
Several core updates are present in the TIC 3.0 artifacts. Distilled in coordination and collaboration with agency stakeholders through several interagency working groups, the modifications introduce new concepts, capabilities, and approaches that established a foundation for TIC 3.0. The following is a summary of the core modifications:

- **Introduction of Trust Models:** Past TIC documentation presented strictly-defined approaches to trust; new TIC documents eschew this "black and white" approach in favor of a more nuanced view that recognizes the reality that the definition of "trust" may vary across specific computing contexts.
- **Introduction of Trust-Based Security Patterns:** Instead of defining its security patterns based on connection classes (e.g., external, internal), TIC 3.0 utilizes a model that defines environments by trust and then describes unique security patterns for connections between environments of various trust levels.
- **Update to the Security Capabilities:** The TIC 3.0 Security Capabilities Handbook features additions, deletions, and modifications of capabilities to reflect a decade's worth of technological evolution, policy and program developments, and stakeholder feedback. The handbook also features new supplemental guidance to support agency implementation of relevant capabilities as well as capability scores to determine their application in various use cases, which are described in greater detail below.
- **Adoption of Risk-Based Approach:** The TIC 3.0 Security Capabilities Handbook discards the "Critical/Recommended" capability prioritization approach utilized in previous versions. The new version assigns scores that are used in conjunction with trust and data sensitivity criteria to determine whether, and the extent to which, security capabilities are applied in each use case.
- **Adoption of Multiple Policy Enforcement Points (PEPs):** 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.
- **Restructure of Documentation Set:** Previously, the TIC Reference Architecture functioned as the primary source of TIC-related guidance. The new structure separates content from the reference architecture into accompanying guidance documents, use cases, and overlays. This approach allows for more agile modifications of all TIC-related guidance (e.g., modifications to individual capabilities will no longer require re-approval of the full RA).
- **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.

6. Key Program Documents

TIC 3.0 documents, listed in Figure 3, 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 catalog of TIC documents is depicted in Figure 3 and described in detail below.

Figure 3: TIC 3.0 Key Program Documents List



Policy Memorandum

Beginning with the policy memorandum, OMB Memorandum 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
- 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 Memorandum M-19-26 requirements into concrete TIC guidance. The guidebook transitions agencies through the modernization effort, providing context on core modifications to the program. It provides historical context and the modernization approach for the program. The guidebook also clarifies the relationship that TIC has to other initiatives, programs, and entities, such as the CSF 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 use cases. The Reference Architecture describes the baseline implementation of TIC 3.0 that follows the past program guidance, pushing all traffic through a physical access point.

Volume 3: Security Capabilities Handbook

Complementary to the RA, the Security Capabilities Handbook features an index of security capabilities applicable to provide updated guidance. The capabilities are derived from the security objectives and as such are mapped to the Cybersecurity Framework. The Security Capabilities Handbook maps the relationship between the CSF, the security objectives, and the TIC capabilities and functions.

Volume 4: TIC Use Case Handbook and Use Cases

The Reference Architecture and the Security Capabilities Handbook create the foundation for the use cases. The use cases provide examples of architectures and provide guidance on the secure implementation and/or configuration of applications, services, and environments. TIC Use Cases are a mechanism to accommodate the secure use of cloud, mobile, and encrypted environments in the Federal Government.

Volume 5: Service Provider Overlay Handbook and Overlays

The Service Provider Overlay Handbook and overlays leverage the expertise of vendor experts to produce technology-specific overlays of TIC-compatible configurations of vendor applications. Agencies can use the overlays to assess the capabilities of the vendors in their environment to understand what level of service to procure and to identify any potential security capability gaps.

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

7. Integrating TIC into a Risk Management Plan

In accordance with OMB Memorandum 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 Memorandum M-19-26 shifts responsibility for compliance with TIC capabilities to the agency. This provision is intended to provide a flexible framework whereby agencies can examine TIC capabilities in the context of the TIC 3.0 Reference Architecture and use cases that meet the business and risk management needs of the agency. Agencies will need to carefully consider and evaluate technologies and implementation approaches offered by system integrators or service providers to ensure that risk can be managed in accordance with thresholds set by the agency.

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 regularly uses terms such as "abstract," "conceptual," "high-level," "typical," "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.

Many cloud service providers (CSPs) 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 CSP is authorized[7]. In the event the CSP is not FedRAMP authorized or in the process of obtaining authorization, agencies are responsible for accreditation and authorization.

[u]se

Service providers are constantly updating and expanding capabilities, especially those related to TIC 3.0. The TIC PMO mapped the capabilities to the NIST CSF and the NIST Special Publication (SP) 800-53 Rev 4. This mapping will facilitate the development of TIC Overlays for several of the more widely used service providers. The TIC overlays will be coordinated with the FedRAMP PMO and updated periodically to further ease the burden on agencies.

8. 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 potential impact of a cybersecurity event. Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected. The objectives are described in Table 2 below; all references to traffic are notional, describing data, connections, etc.

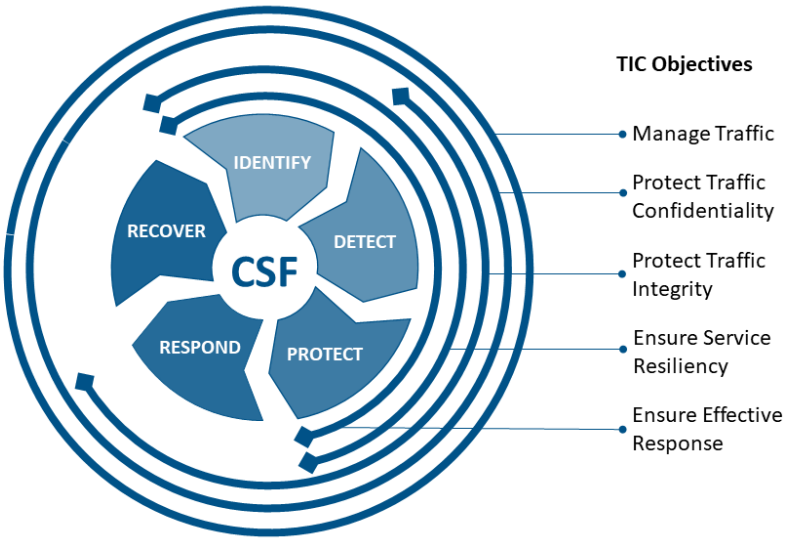
Table 2: TIC 3.0 Security Objectives

Objective	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

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 security objectives are drawn from the NIST CSF[8]. The six objectives can be derived from the five functions of the CSF: Identify, Protect, Detect, Respond, and Recover. The relationship between the CSF and TIC Security Objectives is depicyed in Figure 4. A comprehensive mapping of the CSF, security objectives, and security capabilities can be found in the TIC 3.0 Security Capabilities Handbook.

Figure 4: TIC Lens on the Cybersecurity Framework Functions



9. Use Cases and Overlays

Since 2017, the TIC PMO has been involved in technical discussions with agencies and vendors to explore service provider 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.
- Service providers have significant capabilities that can address the TIC capabilities. Agency architecture or operating needs, customization, and/or additional third-party capabilities may need to be applied to address gaps.
- Service provider capabilities are in a constant state of development to enhance their offerings.
- Overlays of service providers will apply to multiple use cases.

Based on these key observations, the TIC PMO identified a need to decouple the TIC security capabilities from the use cases to support efficient lifecycle management.

[8] "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.

TIC Use Cases provide guidance on the secure implementation and/or configuration of specific platforms, services, and environments. 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 describe the implementation of the capabilities in a given scenario. The use cases will include details on:

- Flow traffic
- Implementation of TIC security capabilities

The SP Overlays contain capability mappings for each service provider independent of the use cases. This approach will allow capabilities to evolve with innovations and outside of use cases update cycle. Overlays will be reviewed and updated to keep pace with industry.

Using this collection of documents, agencies are able to implement TIC into their dispersed environment while meeting all necessary telemetry requirements. In accordance with OMB Memorandum M-19-26, agencies maintain responsibility for implementing the use cases and applicable overlays to ensure their environment is secure.

10. Telemetry Requirements

The *Federal Information Security Modernization Act (FISMA)* 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.

TIC telemetry does not replace or negate the telemetry required by other CISA programs, including NCPS and CDM. Agencies should align the telemetry needs to ensure full compliance. TIC requires agencies to provide self-attestation on their adherence to the program guidance when applicable. Additional information on telemetry requirements is found in Appendix A.

11. Agency Engagement

Each agency is a stakeholder in the TIC initiative and its input is critical to the overall success of the program. The TIC PMO 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 the TIC PMO. 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 TIC PMO; and
- Able to express how the agency wants the TIC initiative to support its activities.

12. TIC Service Options

OMB Memorandum M-19-26 deprecated the original policies that categorized agencies as TICAPs and Service Seeking Agencies. Agencies now have the option to either maintain existing TIC compliance and relationships under the legacy policy construct or leverage the flexibilities in the policy update. Agencies will align with at least one of the following options under the modernized TIC program.

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 vendor-managed 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. 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.

13. TIC and Other Initiatives

TIC 3.0 complements other federal initiatives 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) 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. The ways that agency employees access networks changed completely in the past decade. Consequently, agencies are rethinking their approaches to security to account for employees who telecommute, travel, and use a variety of different devices.

TIC and National Institute of Standards and Technology Zero Trust Architecture

The NIST Zero Trust Architecture (ZTA) principles in SP 800-207 (Draft) 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 TIC 3.0 implementations as the trust of a zone is designated independently of adjacent zones. 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. 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 CSP security 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. 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 aligns with TIC security compliance requirements and supports TIC goals like the reduction and consolidation of external access points across the federal enterprise.

TIC and Continuous Diagnostics and Mitigation

Consistent 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. 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 addressing providing visibility into an agency network, which requires the management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE).

TIC and High Value Assets

High Value Assets (HVA) are those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state-sponsored actor for either direct exploitation or to cause a loss of confidence in the U.S. Government. HVA aligns with TIC with specific regards to trust zones and boundaries. A zone can have cloud, mobile, and interactions between private and public-facing parts of the agency. However, the move to a hybrid cloud for TIC will require those zone boundaries to change, especially with regards to the critical nature of HVAs.

14. 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 Memorandum M-19-26, the TIC 3.0 Reference Architecture, 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.

Appendix A – TIC and NCPS Programs

The TIC and NCPS initiatives are further described in the established by Joint Presidential Directive NSPD-54/HSPD-23; OMB Memorandum M-19-26, Update to the Trusted Internet Connections (TIC) Initiative; and CISA's documentation. 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. § 151(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. § 151(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. § 151, note.

Appendix B – References

LEGISLATION

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

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 – Definitions, Acronyms, and Attributions

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

Cloud Services: Cloud services are a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Control: The amount of authority an agency has over an environment's security policies, procedures and practices.

Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management.

Hybrid TIC Model: An alternative approach to implementing TIC services that blends the use of agency hosted and managed TIC access providers (TICAP) and MTIPS solutions.

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

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

Logical Architecture: A structural design that gives an appropriate level and as much detail as possible without constraining the architecture to a particular technology or environment.

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

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

National Cyber Protection System (NCPS): A system responsible for cyber activity analysis and response that works collaboratively with public, private and international entities to secure cyberspace and America’s cyber assets.

Personal Devices: Devices owned by an employee that is used for work purposes and/or contains the employer’s data.

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

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

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

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

Security Capability: Used to satisfy the security requirements and provide appropriate mission and business protections. Security capabilities are typically defined by bringing together a specific set of safeguards and countermeasures and implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

Trust Zone Diagram: A diagram used to connect the concepts of TIC 3.0—designate trust zones and identify the locations of the PEPs and the MGMT—over a logical architecture

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

Sensitivity: The impact of compromise to an information system's confidentiality, integrity or availability.

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

Software-as-a-Service (SaaS): A software distribution model in which a third-party provider hosts an application and makes it available to customers over the internet.

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

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

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

TIC Initiative: Presidential directive to optimize and standardize the security of individual external network connections currently in use by the Federal Government, to include connections to the internet.

TIC Use Case: A document that identifies the applicable security capabilities and describes the implementation of the capabilities in a given scenario.

Transparency: The degree of visibility an agency has into an environment.

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

Verification: The extent to which an agency can verify an environment's compliance with relevant controls, standards and best practices.

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

Zone: A portion of a network that has specific security requirements.