Trusted Internet Connections 3.0

Vol. 3: Security Capabilities Handbook

December 2019

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Draft

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.

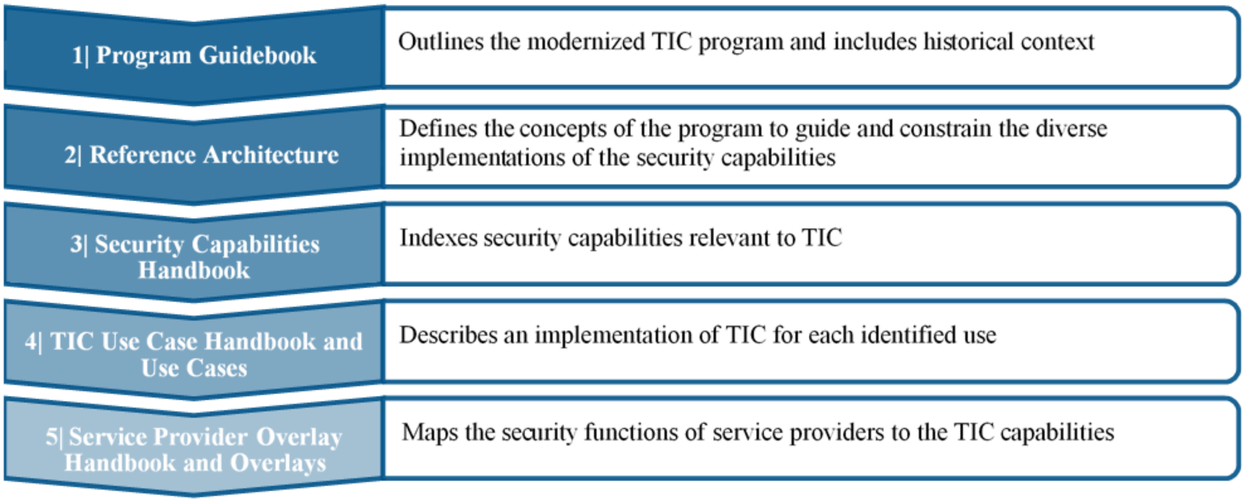
Disclaimer

The Trusted Internet Connections (TIC) 3.0 implementation guidance is described throughout a series of documents. Each document builds on the other and is referenced as sequential volumes. Readers should refer to the first volume, the TIC 3.0 Program Guidebook, as the principal guidance document.

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



1| Program Guidebook — Outlines the modernized TIC program and includes historical context

2| Reference Architecture — Defines the concepts of the program to guide and constrain the diverse implementations of the security capabilities

3| Security Capabilities Handbook — Indexes security capabilities relevant to TIC

4| TIC Use Case Handbook and Use Cases — Describes an implementation of TIC for each identified use

5| Service Provider Overlay Handbook and Overlays — Maps the security functions of service providers to the TIC capabilities

TIC 3.0 Security Capabilities Handbook

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 or multi-boundary 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 Program Guidebook. 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 policy enforcement points, 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 Security Capabilities Handbook

The Security Capabilities Handbook provides a list of deployable security controls, security capabilities, and best practices. The handbook is intended to guide secure implementation and satisfy program requirements within discrete networking environments. The Security Capabilities Handbook offers actionable guidance for employing the principles articulated in the TIC 3.0 Program Guidebook, as well as the secure architecture and components outlined in the TIC 3.0 Reference Architecture. Additionally, the capabilities included in this document can be aligned with service provider overlays to enable deployment of existing and future TIC Use Cases.

The Security Capabilities Handbook enables agencies to apply risk management principles and best practices to protect federal information in various computing scenarios. The trust criteria presented in the TIC 3.0 Reference Architecture can be further applied to an agency’s implementation of a given use case to determine the level of rigor required for each capability. In some cases, the security capabilities may not adequately address residual risks necessary to protect information and systems; agencies are obligated to identify and apply compensating controls or alternatives that provide commensurate protections. Additional collaboration with vendors and service providers is necessary to ensure security requirements are adequately fulfilled, configured, and maintained.

The capabilities presented in this document constitute requirements derived from modern and emerging technologies in addition to requirements articulated in previous TIC documentation. The following selection criteria guides decision-making for including capabilities found in Section 4.

- **Technology Maturity:** Is the underlying technology mature enough to support the adoption of the capability?
- **Sensor Positioning:** Can the capability be positioned to effectively measure performance and security within a network or environment?
- **Policy Enforcement Point (PEP) Deployment:** Can the capability be deployed at a PEP within a given TIC implementation scenario?
- **Scoped to TIC Initiative:** Does the capability's purpose fall within the scope of TIC (i.e., baseline network security, consolidation of trusted connections, address TIC security objectives)?
- **Use Case Applicability:** Does the capability apply to one or more networking scenarios (such as those outlined in TIC Use Cases)?

The Security Capabilities Handbook is intended to keep pace with the evolution of policy and technology. Consequently, this document will be updated periodically to assess existing TIC capabilities against changes in business mission needs, market trends, and the threat landscape.

3. 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 1 below; all references to traffic are notional, describing data, connections, etc.

Table 1: 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 in order to execute another.

4. Security Capabilities List

The capabilities list is composed of two parts:

- **Universal Security Capabilities:** Enterprise-level capabilities that outline guiding principles for TIC Use Cases.
- **Policy Enforcement Point Security Capabilities:** Network-level capabilities that inform technical implementation for relevant use cases.

The capabilities are intended to fulfill the TIC Objectives outlined in Section 3.

4.1 Universal Security Capabilities

Universal capabilities are enterprise-level capabilities that outline guiding principles for TIC Use Cases and apply across use cases. Agencies have the discretion to determine the level of rigor necessary for applying universal capabilities based on federal guidelines and risk tolerance. The table below provides: (1) a list of the universal security capabilities, (2) a description of each capability, and (3) a mapping of each capability to relevant NIST Cybersecurity Framework (CSF) categories. While universal capabilities are broadly applicable, certain use cases may provide unique guidance on specific capabilities where necessary.

Table 2: Universal Security Capabilities

Capability	Description	NIST CSF Mapping
Backup and Recovery	Keeping copies of configuration and data, as needed, to allow for the quick restoration of service in the event of malicious incidents, system failures or corruption.	PR.IP, PR.DS, RS.MI, RC.RP
Central Log Management with Analysis	Storing telemetry needed to discover and respond to malicious activity in a manner that facilitates security analysis and data fusion.	ID.AM, PR.PT, DE.AE, RS.AN
Configuration Management	Implementing a formal plan for documenting, and managing changes to the environment, and monitoring for deviations.	ID.BE, PR.DS, PR.IP, PR.MA
Incident Response Plan and Incident Handling	Documenting and implementing a set of instructions or procedures to detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and systems.	ID.GV, ID.RA, PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI

Inventory	Developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	ID.AM, PR.DS, PR.AC, PR.DS, PR.IP
Least Privilege	Designing the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	ID.AM, PR.AC, PR.IP, PR.PT, DE.CM
Secure Administration	Performing administrative tasks in a secure manner, using secure protocols.	PR.MA
Strong Authentication	Verifying the identity of users, devices or other entities through rigorous means (e.g. multi-factor authentication) before granting access.	PR.AC
Time Synchronization	Coordinating clocks on all systems (e.g. servers, workstations, network devices) to enable accurate comparison of timestamps between systems.	PR.IP
Vulnerability Assessment	Proactively working to discover vulnerabilities, including the use of both active and passive means of discovery, and taking action to mitigate discovered vulnerabilities.	ID.RA, PR.IP DE.AE, DE.CM, DE.DP
Auditing and Accounting	Capturing business records, including logs and other telemetry, and making them available for auditing and accounting as required.	ID.SC, PR.AC, PR.PT
Resilience	Ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	ID.BE, PR.PT
Enterprise Threat Intelligence	Obtaining threat intelligence from private and government sources, and implementing mitigations for the identified risks.	ID.RA, DE.AE, DE.CM, DE.DP
Situational Awareness	Maintaining effective awareness, both current and historical, across all components.	ID.AM, ID.RA, PR.DS, PR.IP, DE.AE, DE.CM, DE.DP, RS.CO
Dynamic Threat Discovery	Using dynamic approaches (e.g. heuristics, baselining, etc.) to discover new malicious activity.	ID.RA, DE.AE, DE.CM, DE.DP

Policy Enforcement Parity	Consistently applying security protections and other policies, independent of the conveyance mechanism used.	PR.DS, PR.IP, PR.MA
Effective Use of Shared Services	Employing shared services, where applicable, that can be individually tailored, measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external as well as internal to the service provider.	ID.AM, ID.GV, ID.RM, ID.SC, PR.AT, RS.CO
Integrated Desktop, Mobile, and Remote Policies	Defining polices such that they apply to a given agency entity no matter its location.	ID.AM, PR.AC, PR.DS, PR.IP, PR.MA

4.2 Policy Enforcement Point Capabilities

Policy Enforcement Point (PEP) Capabilities are network-level capabilities that inform technical implementation for relevant use cases. PEP Capabilities are divided into eight groups and fulfilled by applications, devices, or services identified in TIC Use Cases and TIC Overlays. The eight PEP capability groups correspond to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- DNS,
- Intrusion Detection, and
- Enterprise.

The PEP capability groups listing is not exhaustive. Additional groups may be developed to reflect new use cases. The following tables provide: (1) a list of PEP capabilities, (2) a description of each capability, and (3) a mapping to relevant NIST CSF categories.

Table 3: Policy Enforcement Point Security Capabilities for Files

Files PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
Anti-malware	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.	PR.DS, PR.PT, DE.CM, DE.DP RS.MI
Content Disarm & Reconstruction	Content Disarm & Reconstruction technology detects the presence of unapproved active content and facilitates its removal.	PR.PT, DE.CM, DE.DP
Detonation Chamber	Detonation Chambers facilitate the detection of malicious code through the use of protected and isolated execution environments to analyze the files.	DE.CM, DE.DP RS.AN, RS.MI

Table 4: Policy Enforcement Point Security Capabilities for Email

Email PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
Anti-phishing Protections	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	PR.AT, PR.PT, DE.CM
Anti-SPAM Protections	Anti-SPAM protections detect and quarantine instances of SPAM.	PR.PT, DE.CM
Authenticated Received Chain	Authenticated Received Chain allows for an intermediary, like a mailing list or forwarding service, to sign its own authentication of the original email, allowing downstream entities to accept the intermediary's authentication even if the email was changed.	PR
Data Loss Prevention	Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data	PR.DS
DMARC for Incoming Email	DMARC protections authenticate incoming email according to the DMARC email authentication protocol defined in RFC 7489.	PR.PT, PR.IP
DMARC for Outgoing Email	DMARC protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures. The DMARC email authentication protocol is defined in RFC4789.	PR.PT, PR.IP

Encryption for Email Transmission	Email Services are configured to use encrypted connections, when possible, when interacting with Clients and other Email Servers.	PR.PT, PR.DS
Malicious URL Protections	Malicious URL Protections detect malicious URLs in emails and prevent users from accessing them.	PR.PT, DE.CM
URL Click-Through Protection	URL Click-Through Protections ensures that when a URL from an email is clicked, the requester is directed to a protection that verifies the security of the URL destination before permitting access.	PR.PT, DE.CM
NCPS E3A Protections	NCPS E3A is an intrusion prevention capability, provided by DHS, that includes an Email Filtering security service.	PR.PT, DE.CM

Table 5: Policy Enforcement Point Security Capabilities for Web

Web PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
Break and Inspect	Break-and-Inspect systems terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.	PR.PT, DE.CM
Active Content Mitigation	Active Content Mitigation protections detect the presence of unapproved active content and facilitate its removal.	PR.PT, DE.CM
Certificate Blacklisting	Certificate Blacklisting protections prevent communication with entities that use a set of known bad certificates.	PR.PT, DE.CM
Certificate Consensus	Certificate Consensus provides a comparison of all observed certificates in use for consistency and preventing use of inconsistent credentials.	PR.AC, DE.CM
Content Filtering	Content Filtering protections detect the presence of unapproved content and facilitate its removal.	PR.PT, DE.CM, DE.DP
Authenticated Proxy	Authenticated Proxies require entities to authenticate with the proxy before making use of it, enabling user, group, and location-aware security controls.	PR.AC

Data Loss Prevention	Data Loss Prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS
DNS-over-HTTPS Filtering	DNS-over-HTTPS filtering prevents entities from using the DNS-over-HTTPS protocol, possibly evading DNS-based protections.	PR.PT, DE.CM
RFC Compliance Enforcement	RFC Compliant Enforcement technologies ensure that traffic complies with protocol definitions.	PR.PT
Domain Category Filtering	Domain Category Filtering technologies allow for classes of domains (e.g. banking, medical) to receive a different set of security protections.	PR.AC, PR.IP
Domain Reputation Filter	Domain Reputation Filtering protections are a form of Domain Blacklisting based on a domain's reputation, as defined by either the agency or an external entity.	PR.PT
Bandwidth Control	Bandwidth Control technologies allow for limiting the amount of bandwidth used by different classes of domains.	PR.PT
Malicious Content Filtering	Malicious Content Filtering protections detect the presence of malicious content and facilitate its removal.	PR.DS, PR.PT, DE.CM
Access Control	Access Control technologies allow an agency to define policies concerning what entities may perform.	PR.AC

Table 6: Policy Enforcement Point Security Capabilities for Networking

Networking PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
Network Access Controls	Network Access Control protections prevent the ingest or transiting of unauthorized network traffic.	PR.AC, PR.IP, DE.CM
IP Blacklisting	IP Blacklisting protections prevent the ingest or transiting of traffic received from or destined to a blacklisted IP address.	PR.PT, DE.CM
Host Containment	Host Containment protections enable a network to revoke a host's access to the network.	PR.AC, PR.IP, PR.PT
Network Segmentation	Network Segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	PR.AC
Microsegmentation	Microsegmentation divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.	PR.AC, PR.DS, PR.IP, PR.PT

Table 7: Policy Enforcement Point Security Capabilities for Resiliency

Resiliency PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
DDoS Protections	DDoS protections mitigate the effects of distributed denial of service attacks.	PR.PT
Elastic Expansion	Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.	ID.AM, PR.DS
Regional Delivery	Regional Delivery technologies enable the deployment of agency services across geographically diverse locations.	ID.AM, PR.AC, PR.DS

Table 8: Policy Enforcement Point Security Capabilities for DNS

DNS PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
DNS Blackholing	DNS Blackholing protections are a form of blacklisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.	PR.PT
DNSSEC for Agency Clients	DNSSEC protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated.	PR.PT
DNSSEC for Agency Domains	DNSSEC protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution the domain names.	PR.PT

Table 9: Policy Enforcement Point Security Capabilities for Intrusion Detection

Intrusion Detection PEP Security Capabilities

Capability	**Description**	**NIST CSF Mapping**
Endpoint Detection and Response	Endpoint Detection and Response tools combine endpoint and network event data to aid in the detection of malicious activity.	DE.AE, DE.CM, RS.AN
Intrusion Protection Systems (IPS)	Intrusion Protection Systems detect malicious activity, attempt to stop the activity, and report the activity.	DE.AE, DE.CM, DE.DP, RS.AN
Adaptive Access Control	Adaptive Access Control technologies factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.	PR.AC, DE.CM
Deception Platforms	Deception Platform technologies provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.	PR.PT, DE.AE, RS.AN
Certificate Transparency Log Monitoring	Certificate Transparency Log Monitoring allows agencies to discover when new certificates are issued for agency domains.	DE.CM

Table 10: Policy Enforcement Point Security Capabilities for Enterprise

Enterprise PEP Security Capabilities

Capability	Description	NIST CSF Mapping
Security Orchestration, Automation, and Response (SOAR)	Security Orchestration, Automation and Response tools define, prioritize and automate the response to security incidents.	DE.AE, DE.CM, DE.DP, RS.CO, RS.AN, RC.RP
Shadow IT Detection	Shadow IT Detection systems detect the presence of unauthorized software and systems in use by an agency.	PR.IP, PR.MA, DE.CM
VPN	Virtual Private Network solutions provide a secure communications mechanism between networks that may traverse across unprotected or public networks.	PR.AC, PR.DS, PR.IP, PR.MA, PR.PT

5. Conclusion

This document lists the TIC security capabilities. TIC Use Cases will reference capabilities from this handbook and will provide guidance on how to deploy these capabilities within the context of a unique use case. TIC Overlays will provide mappings from these capabilities to vendor-specific tools and services. Over time, this handbook will be updated and will be informed by TIC pilot activities, TIC Use Cases, emerging technologies, and threat insight.

Appendix A – 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.