Trusted Internet Connections 3.0

TIC Core Guidance Volume 3:
Security Capabilities Catalog

October 2021

Version 2.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Revision History

The version number will be updated as the document is modified. This document will be updated as needed to reflect modern security practices and technologies.

Table 1: Revision History

Version	Date	Revision Description	Sections/Pages Affected
Draft	December 2019	Initial Release	All
1.0	July 2020	Response to RFC Feedback	All
1.1	April 2021	Updated Figure 2 for clarity. Modified the format of universal capability descriptions. Altered the names of security capabilities to remove acronyms.	Pg. 4 Pg. 6-8 Pg. 9-17
2.0	October 2021	Added a "capability identifiers" column to the security capabilities tables Added the following security capabilities: User Awareness and Training, Domain Name Monitoring, Application Container, Remote Desktop Access	Pg. 6-17 Pg. 8, 14, 16

Reader's Guide

The Trusted Internet Connections (TIC) initiative is defined through key documents that describe the directive, the program, the capabilities, the implementation guidance, and capability mappings. Each document has an essential role in describing TIC and its implementation. The documents provide an understanding of how changes have led to the latest version of TIC and why those changes have occurred. The documents go into high-level technical detail to describe the exact changes in architecture for TIC 3.0. The documents are additive; each builds on the other like chapters in a book. As depicted in Figure 1, the documents should be referenced in order and to completion to gain a full understanding of the modernized initiative.

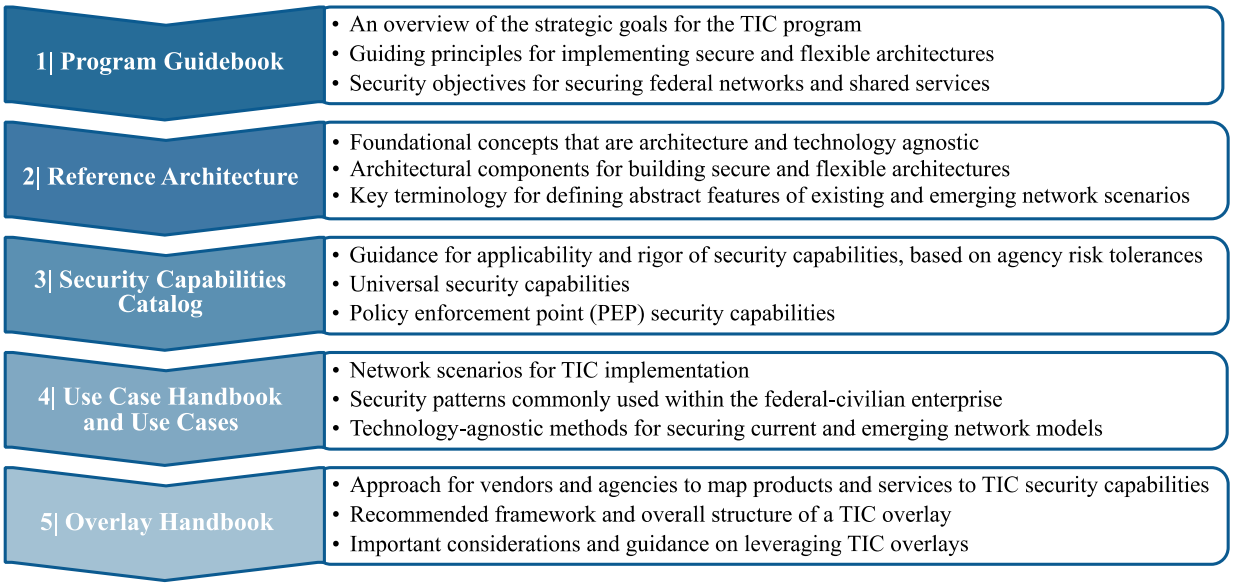

Figure 1: TIC 3.0 Guidance Snapshot

TIC 3.0 Security Capabilities Catalog

Table of Contents

List of Figures

List of Tables

1. Introduction

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

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

1.1 Key Terms

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.

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 expire in Fiscal Year (FY) 2023.

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

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

Security Capability: A combination of mutually-reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).[2] Security capabilities help to define protections for information being processed, stored, or transmitted by information systems.

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

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

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

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

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

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

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

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

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

2. Purpose of the Security Capabilities Catalog

The *TIC 3.0 Security Capabilities Catalog* (Security Capabilities Catalog) provides a list of deployable security controls, security capabilities, and best practices. The catalog is intended to guide secure implementation and help agencies satisfy program requirements within discrete networking environments. The security capabilities included in this document can be aligned with TIC overlays to enable deployment of existing and future TIC use cases.

The Security Capabilities Catalog helps agencies to apply risk management principles and best practices to protect federal information in various computing scenarios. The trust considerations 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 security 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 is necessary to ensure security requirements are adequately fulfilled, configured, and maintained.

The security capabilities presented in this document are derived from modern and emerging technologies in addition to requirements articulated in previous TIC documentation. The following selection criteria guides decision-making for including security 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 Deployment:** Can the capability be deployed at a policy enforcement point (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?
- **Goal-Based:** Does the capability specify a goal to be achieved rather than specifying how to achieve a goal?

The list of security capabilities in this catalog does not represent an exhaustive listing of security capabilities; many otherwise valuable security capabilities are excluded by the selection criteria above. For example, while supply chain risk is an important security consideration, it falls outside the scope of the TIC initiative.

The Security Capabilities Catalog is intended to keep pace with the evolution of policy and technology. Consequently, this document will be updated periodically to assess existing TIC security capabilities against changes in business mission needs, market trends, and 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 are intended to limit the likelihood of a cybersecurity event. Agencies are granted discretion to apply the objectives at a level commensurate to the type of resources being protected.

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

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.

The TIC objectives, described in Table 2, are intended to set expectations for architectures, guide implementation, and establish clear goals at the network level. The term "traffic" in the TIC objectives refers to network traffic or data in transit between trust zones or stored at either or both trust zones.

Table 2: TIC 3.0 Security Objectives

Objective[3]	Description
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny

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

Objective[3]	Description
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 can be mapped to the five functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[4]: Identify, Protect, Detect, Respond, and Recover. The relationship between the CSF and TIC security objectives is depicted in Figure 2. Furthermore, the TIC security capabilities are mapped to the NIST CSF in the Security Capabilities Catalog in the following sections. This mapping will facilitate the development of TIC overlays for several of the more widely used vendors.

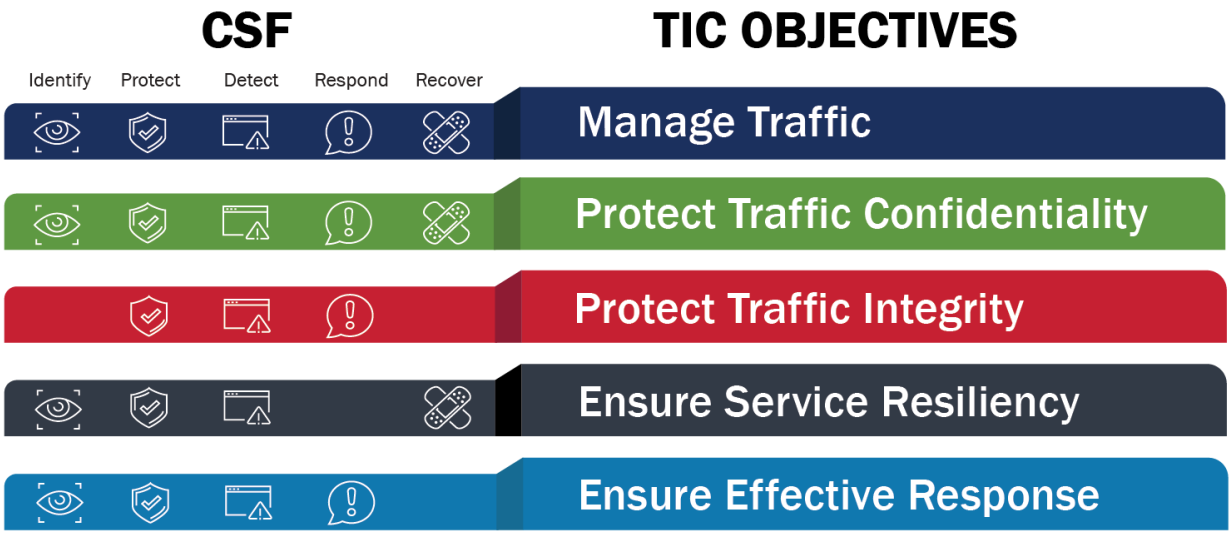

Figure 2: TIC Lens on the Cybersecurity Framework Functions

[4] "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.

4. Security Capabilities List

The security capabilities list is composed of two parts.

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

The security capabilities are intended to fulfill the TIC objectives outlined in Section 3. The Security Capabilities Catalog is not intended to be an exhaustive listing, and it does not provide detailed guidance about how to deploy each capability. The purpose of the Security Capabilities Catalog is to provide goals to be achieved, not detailed guidance on how to accomplish these goals. As such, the choice of which solution or solutions to employ is left for each agency to determine, as they balance application and rigor of security capabilities with their risk tolerance.

Security capabilities can be achieved using agency-hosted solutions, leveraging offerings from vendors, consolidating disparate services into federated options, employing centralized management tools, or any combination thereof. While the choice of which solution or solutions to employ is left to the agency based upon their needs, care should be taken to ensure PEP parity. Once an agency determines that a particular security capability is required to protect their network or data, the agency needs to make sure that security capability is implemented at all access points to the network or data.

With respect to telemetry, both CISA and the agencies themselves require visibility, both relying on common data sources. Since visibility requirements will often align, the same telemetry may be used for both CISA and agency purposes (if desired) to simplify collection. Whereas previously a 24-hour packet capture was required, in this iteration of TIC there are no longer any explicit telemetry collection requirements specified related to duration or timeliness. Agencies remain free to address any unique telemetry requirements beyond those required by CISA.

4.1 Universal Security Capabilities

Universal security capabilities are enterprise-level capabilities that outline guiding principles for TIC use cases. Universal security capabilities are selected to be broadly applicable; the same list of capabilities apply to every use case. However, certain use cases may provide unique guidance on specific capabilities where necessary.

Agencies have significant discretion regarding how to meet the individual security capabilities and address their particular needs. Agencies are free to determine the level of rigor necessary for applying universal capabilities based on federal guidelines and their risk tolerance. While it is expected that agencies may often be able to employ a common solution to fulfill multiple roles or serve multiple purposes, the selection of an appropriate set of solutions is left to each agency.

Table 3 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 CSF categories.

Table 3: Universal Security Capabilities

Universal Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Backup and Recovery	3.UNI.BRECO	Backup and recovery entails 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.	ID.BE, PR.IP, PR.DS, RS.MI, RC.RP
Central Log Management with Analysis	3.UNI.CLMAN	Central log management with analysis is the collection, storage, and analysis of telemetry, where the collection and storage are designed to facilitate data fusion and where the security analysis aids in discovery and response to malicious activity.	ID.AM, PR.PT, DE.AE, RS.AN
Configuration Management	3.UNI.CMANA	Configuration management is the implementation of a formal plan for documenting and managing changes to the environment, and monitoring for deviations, preferably automated.	ID.BE, PR.DS, PR.IP, PR.MA
Incident Response Planning and Incident Handling	3.UNI.IRPIH	Incident response planning and incident handling is the documentation and implementation of a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.	ID.GV, ID.RA, PR.IP, DE.DP, DE.AE, RS.RP, RS.CO, RS.AN, RS.MI
Inventory	3.UNI.INVENT	Inventory entails 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 restricted from gaining access.	ID.AM, PR.AC, PR.DS, PR.IP
Least Privilege	3.UNI.LPRIV	Least privilege is a design principle whereby 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	3.UNI.SADMI	Secure administration entails performing administrative tasks in a secure manner, using secure protocols.	PR.MA
Strong Authentication	3.UNI.SAUTH	Strong authentication verifies the identity of users, devices, or other entities through rigorous means (e.g., multi-factor authentication) before granting access.	PR.AC

Capability	Capability Identifier	Description	NIST CSF Mapping
Time Synchronization	3.UNI.TSYNC	Time synchronization is the coordination of system (e.g., servers, workstations, network devices) clocks to minimize the difference between system clock times and enable accurate comparison of timestamps between systems.	PR.IP
Vulnerability Management	3.UNI.VMANG	Vulnerability management is the practice of proactively working to discover vulnerabilities by including the use of both active and passive means of discovery and by taking action to mitigate discovered vulnerabilities.	ID.RA, PR.IP DE.AE, DE.CM, DE.DP
Patch Management	3.UNI.PMANA	Patch management is the identification, acquisition, installation, and verification of patches for products and systems.	ID.AM, PR.IP, PR.MA
Auditing and Accounting	3.UNI.AACCO	Auditing and accounting includes capturing business records (e.g., logs and other telemetry), making them available for auditing and accounting as required, and designing an auditing system that considers insider threat (e.g., separation of duties violation tracking) such that insider abuse or misuse can be detected.	ID.SC, PR.AC, PR.PT
Resilience	3.UNI.RESIL	Resilience entails ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.	ID.BE, PR.PT
Enterprise Threat Intelligence	3.UNI.ETINT	Enterprise threat intelligence is the usage of threat intelligence from private or government sources to implement mitigations for the identified risks.	ID.RA, DE.AE, DE.CM, DE.DP
Situational Awareness	3.UNI.SAWAR	Situational awareness is 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	3.UNI.DTDIS	Dynamic threat discovery is the practice of using dynamic approaches (e.g., heuristics, baselining, etc.) to discover new malicious activity.	ID.RA, DE.AE, DE.CM, DE.DP
Policy Enforcement Parity	3.UNI.PEPAR	Policy enforcement parity entails consistently applying security protections and other policies, independent of the communication mechanism, forwarding path, or endpoints used.	PR.DS, PR.IP, PR.MA

Capability	Capability Identifier	Description	NIST CSF Mapping
Effective Use of Shared Services	3.UNI.EUSSE	Effective use of shared services means that shared services are employed, where applicable, and individually tailored and measured to independently validate service conformance, and offer effective protections for tenants against malicious actors, both external and internal to the service provider.	ID.AM, ID.GV, ID.RM, ID.SC, PR.AT, RS.CO
Integrated Desktop, Mobile, and Remote Policies	3.UNI.IDMRP	This entails the definition and enforcement of policies that apply to a given agency entity independent of its location.	ID.AM, PR.AC, PR.DS, PR.IP, PR.MA
User Awareness and Training	3.UNI.UATRA	User awareness and training entails that all users are informed of their roles and responsibilities and appropriate cybersecurity education is provisioned to enable users to perform their duties in a secure manner.	ID.AM, ID.BE, ID.GV, PR.AT, RS.CO

4.2 Policy Enforcement Point Capabilities

PEP security capabilities are network-level capabilities that inform the technical implementation for relevant use cases. In contrast to the universal security capabilities, which are expected to apply in each use case, PEP security capabilities may or may not be applicable based on the use case scope. PEP security capabilities are divided into groups around shared themes.

The PEP security capability groups listing is not exhaustive. Additional groups may be developed to reflect new use cases. Each PEP security capability group table provides the following: (1) a list of PEP capabilities, (2) a description of each capability, and (3) a mapping to relevant NIST CSF categories. The PEP capability groups correspond to the following security functions:

- Files,
- Email,
- Web,
- Networking,
- Resiliency,
- Domain Name System (DNS),
- Intrusion Detection,
- Enterprise,
- Unified Communications and Collaboration (UCC), and
- Data Protection.

Table 4: Files PEP Security Capabilities

Files PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Anti-malware	3.PEP.FI.AMALW	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

Capability	Capability Identifier	Description	NIST CSF Mapping
Content Disarm and Reconstruction	3.PEP.FI.CDREC	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.	PR.PT, DE.CM, DE.DP
Detonation Chamber	3.PEP.FI.DCHAM	Detonation chambers facilitate the detection of malicious code using protected and isolated execution environments to analyze the files.	DE.CM, DE.DP RS.AN, RS.MI
Data Loss Prevention	3.PEP.FI.DLPRE	Data loss prevention (DLP) technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS

Table 5: Email PEP Security Capabilities

Email PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Anti-phishing Protections	3.PEP.EM.APPRO	Anti-phishing protections detect instances of phishing and prevent users from accessing them.	PR.AT, PR.PT, DE.CM
Anti-spam Protections	3.PEP.EM.ASPRO	Anti-spam protections detect and quarantine instances of spam.	PR.PT, DE.CM
Authenticated Received Chain	3.PEP.EM.ARCHA	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.AC
Data Loss Prevention	3.PEP.EM.DLPRE	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS
Domain Signature Verification for Incoming Email	3.PEP.EM.DSVIE	Domain signature verification protections authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC) email authentication protocol defined in Request for Comments (RFC) 7489[5].	PR.PT, PR.IP

[5] "Domain-based Message Authentication, Reporting, and Conformance Request for Comments: 7489," Internet Engineering Task Force (2015). https://tools.ietf.org/html/rfc7489.

Capability	Capability Identifier	Description	NIST CSF Mapping
Domain Signatures for Outgoing Email	3.PEP.EM.DSOEM	Domain signature protections facilitate the authentication of outgoing email by signing the emails and ensuring that external parties may validate the email signatures according to the DMARC email authentication protocol that is defined in RFC 7489.	PR.PT, PR.IP
Encryption for Email Transmission	3.PEP.EM.EETRA	Email services are configured to use encrypted connections, when possible, for communications between clients and other email servers.	PR.PT, PR.DS
Malicious Link Protections	3.PEP.EM.MLPRO	Malicious link protections detect malicious links in emails and prevent users from accessing them.	PR.PT, DE.CM
Link Click-through Protection	3.PEP.EM.LCTPR	Link click-through protections ensure that when a link from an email is clicked, the requester is directed to a protection that verifies the security of the link destination before permitting access.	PR.PT, DE.CM
EINSTEIN 3 Accelerated Email Protections	3.PEP.EM.E3AEP	EINSTEIN 3 Accelerated (E^3A)[6] is an intrusion prevention capability offered by NCPS, provided by CISA, that includes an email filtering security service.	PR.PT, DE.CM

Table 6: Web PEP Security Capabilities

Web PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Break and Inspect	3.PEP.WE.BINSP	Break and Inspect systems, or encryption proxies, 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	3.PEP.WE.ACMIT	Active content mitigation protections detect the presence of unapproved active content and facilitate its removal.	PR.PT, DE.CM

[6] "EINSTEIN 3 Accelerated," Cybersecurity and Infrastructure Security Agency (2013). https://www.cisa.gov/publication/einstein-3-accelerated.

Capability	Capability Identifier	Description	NIST CSF Mapping
Certificate Denylisting	3.PEP.WE.CDENY	Certificate denylisting protections prevent communication with entities that use a set of known bad certificates.	PR.PT, DE.CM
Content Filtering	3.PEP.WE.CFILT	Content filtering protections detect the presence of unapproved content and facilitate its removal or denial of access.	PR.PT, DE.CM, DE.DP
Authenticated Proxy	3.PEP.WE.APROX	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	3.PEP.WE.DLPRE	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS
Domain Resolution Filtering	3.PEP.WE.DRESF	Domain resolution filtering prevents entities from using the DNS-over- Hypertext Transfer Protocol Secure (HTTPS), or DoH, domain resolution protocol, possibly evading DNS-based protections.	PR.PT, DE.CM
Protocol Compliance Enforcement	3.PEP.WE.PCENF	Protocol compliance enforcement technologies ensure that traffic complies with protocol definitions, documented by the Internet Engineering Task Force (IETF)[7].	PR.PT
Domain Category Filtering	3.PEP.WE.DCFIL	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 Filtering	3.PEP.WE.DREPF	Domain reputation filtering protections are a form of domain denylisting based on a domain's reputation, as defined by either the agency or an external entity.	PR.PT
Bandwidth Control	3.PEP.WE.BCONT	Bandwidth control technologies allow for limiting the amount of bandwidth used by different classes of domains.	PR.PT
Malicious Content Filtering	3.PEP.WE.MCFIL	Malicious content filtering protections detect the presence of malicious content and facilitate its removal.	PR.DS, PR.PT, DE.CM

[7] "RFCs," Internet Engineering Task Force (2021). https://www.ietf.org/standards/rfcs/

Capability	Capability Identifier	Description	NIST CSF Mapping
Access Control	3.PEP.WE.ACONT	Access control technologies allow an agency to define policies limiting what actions may be performed by connected users and entities.	PR.AC

Table 7: Networking PEP Security Capabilities

Networking PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Access Control	3.PEP.NE.ACONT	Access control protections prevent the ingress, egress, or transmission of unauthorized network traffic.	PR.AC, PR.IP, DE.CM
Internet Address Denylisting	3.PEP.NE.IADEN	Internet address denylisting protections prevent the ingest or transiting of traffic received from or destined to a denylisted internet address.	PR.PT, DE.CM
Host Containment	3.PEP.NE.HCONT	Host containment protections enable a network to revoke or quarantine a host's access to the network.	PR.AC, PR.IP, PR.PT
Network Segmentation	3.PEP.NE.NSEGM	Network segmentation separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.	PR.AC
Micro-segmentation	3.PEP.NE.MICRO	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 8: Resiliency PEP Security Capabilities

Resiliency PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Distributed Denial of Service Protections	3.PEP.RE.DDSPR	Distributed Denial of Service (DDoS) protections mitigate the effects of distributed denial of service attacks.	PR.PT
Elastic Expansion	3.PEP.RE.EEXPS	Elastic expansion enables agencies to dynamically expand the resources available for services as conditions require.	ID.AM, PR.DS
Regional Delivery	3.PEP.RE.RDELI	Regional delivery technologies enable the deployment of agency services across geographically diverse locations.	ID.AM, PR.AC, PR.DS

Table 9: Domain Name System PEP Security Capabilities

Domain Name System PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Domain Name Sinkholing	3.PEP.DO.DNSIN	Domain name sinkholing protections are a form of denylisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.	PR.PT
Domain Name Verification for Agency Clients	3.PEP.DO.DNVAC	Domain name verification protections ensure that domain name lookups from agency clients, whether for internal or external domains, are validated according to Domain Name System Security Extensions (DNSSEC).	PR.PT
Domain Name Validation for Agency Domains	3.PEP.DO.DNVAD	Domain name validation protections ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution to the domain names.	PR.PT
Domain Name Monitoring	3.PEP.DO.DNMON	Domain name monitoring allows agencies to discover the creation of or changes to agency domains.	ID.RA, PR.AC, DE.CM

Capability	Capability Identifier	Description	NIST CSF Mapping
EINSTEIN 3 Accelerated Domain Name Protections	3.PEP.DO.E3ADN	E^3A is an intrusion prevention capability offered by NCPS, provided by CISA, that includes a DNS sinkholing security service.	PR.PT

Table 10: Intrusion Detection PEP Security Capabilities

Intrusion Detection PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Endpoint Detection and Response	3.PEP.IN.EDRES	Endpoint detection and response (EDR) tools combine endpoint and network event data to aid in the detection of malicious activity.	DE.AE, DE.CM, RS.AN
Intrusion Detection and Prevention Systems	3.PEP.IN.IDSY	Intrusion detection systems detect and report malicious activity. Intrusion prevention systems attempt to stop the activity.	DE.AE, DE.CM, DE.DP, RS.AN
Adaptive Access Control	3.PEP.IN.AACON	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	3.PEP.IN.DPLAT	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	3.PEP.IN.CTLMO	Certificate transparency log monitoring allows agencies to discover when new certificates are issued for agency domains.	DE.CM

Table 11: Enterprise PEP Security Capabilities

Enterprise PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Security Orchestration, Automation, and Response	3.PEP.EN.SOARE	Security Orchestration, Automation, and Response (SOAR) tools define, prioritize, and automate the response to security incidents.	DE.AE, DE.CM, DE.DP, RS.CO, RS.AN, RC.RP
Shadow Information Technology Detection	3.PEP.EN.SITDE	Shadow information technology (IT) detection systems detect the presence of unauthorized software and systems in use by an agency.	PR.IP, PR.MA, DE.CM
Virtual Private Network	3.PEP.EN.VPNET	Virtual private network (VPN) 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
Application Container	3.PEP.EN.ACONT	A virtualization approach in which applications are isolated to a known set of dependencies, access methods, and interfaces.	PR.AC, PR.DS
Remote Desktop Access	3.PEP.EN.RDACC	Remote desktop access solutions provide a mechanism for connecting to and controlling a remote physical or virtual computer.	PR.AC, PR.DS, PR.PT

Table 12: Unified Communications and Collaboration PEP Security Capabilities

Unified Communications and Collaboration PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Identity Verification	3.PEP.UN.IVERI	Identity verification ensures that access to the virtual meeting is limited to appropriate individuals. Waiting room features, where the meeting host authorizes vetted individuals to join the meeting, can also be utilized.	PR.AC

Capability	Capability Identifier	Description	NIST CSF Mapping
Encrypted Communication	3.PEP.UN.ECOMM	Communication between virtual meeting participants and any data exchanged is encrypted at rest and in transit. Some UCC offerings support end-to-end encryption, where encryption is performed on the clients and can only be decrypted by the other authenticated participants and cannot be decrypted by the UCC vendor.	PR.PT, PR.DS
Connection Termination	3.PEP.UN.CTERM	Connection termination mechanisms ensure the meeting host can positively control participation through inactivity timeouts, on-demand prompts, unique access codes for each meeting, host participant eviction, and even meeting duration limits.	PR.AC, PR.IP, PR.AT
Data Loss Prevention	3.PEP.UN.DLPRE	Mechanisms should be implemented to control the sharing of information between UCC participants, intentional or incidental. This may be integrated into additional agency DLP technologies and can include keyword matching, attachment file type or existence prohibitions, attachment size limitations, or even audio/visual filters.	PR.DS

Table 13: Data Protection PEP Security Capabilities

Data Protection PEP Security Capabilities

Capability	Capability Identifier	Description	NIST CSF Mapping
Access Control	3.PEP.DA.ACONT	Access control technologies allow an agency to define policies concerning the allowable activities of users and entities to data and resources.	PR.AC, PR.IP, DE.CM
Protections for Data at Rest	3.PEP.DA.PDRES	Data protection at rest aims to secure data stored on any device or storage medium.	PR.DS
Protections for Data in Transit	3.PEP.DA.PDTRA	Data protection in transit, or data in motion, aims to secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.	PR.DS
Data Loss Prevention	3.PEP.DA.DLPRE	DLP technologies detect instances of the exfiltration, either malicious or accidental, of agency data.	PR.DS

Capability	Capability Identifier	Description	NIST CSF Mapping
Data Access and Use Telemetry	3.PEP.DA.DAUTE	This entails identifying agency sensitive data stored, processed, or transmitted, including those located at a service provider and enforcing detailed logging for access or changes to sensitive data.	ID.AM, PR.AC, PR.DS, PR.PT, DE.AE, DE.CM

5. Conclusion

This document lists the TIC security capabilities. TIC use cases will reference security capabilities from this catalog 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 security capabilities to vendor-specific tools and services. Over time, this catalog will be updated and will be informed by TIC pilot activities, TIC use cases, emerging technologies, and threat insight.

Appendix A – Glossary and Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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