U.S. General Services Administration
Federal Acquisition Service
Information Technology Category

Moving IT Modernization Forward with Enterprise Infrastructure Solutions (EIS) and Trusted Internet Connections (TIC) 3.0

Issued by:

General Services Administration

Office of Enterprise Technology Solutions

1800 F St NW

Washington, DC 20405

https://gsa.gov/eis

Version 1.4

June 2021

Table of Contents

Moving IT Modernization Forward with EIS and TIC 3.0

1.0 What is TIC 3.0?

With the change by the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) Trusted Internet Connections (TIC) program office from TIC 2.2 to TIC 3.0, many agencies have been wondering what this means. In short, TIC 3.0 lifts the restrictions of forcing an agency's Internet connections to be centralized to common exit and entry points and provides the flexibility to allow the agency to make their own risk-based decision on how their networks can be constructed to best meet their mission needs securely.

TIC 3.0 was introduced on September 12, 2019 when OMB Memorandum (M) 19-26: Update to the Trusted Internet Connections (TIC) Initiative was released. The earlier versions of the TIC initiative sought to consolidate federal networks and standardize perimeter security for the federal enterprise. As outlined in OMB M-19-26, the modernized version of the TIC initiative expands upon the original to drive security standards and leverage advances in technology as agencies modernize to more mobile and cloud environments. The updated OMB policy signals a shift in the focus of the TIC initiative from compliance driven requirements towards architecture, strategy, visibility, and flexibility. The TIC 3.0 focus is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications.

The TIC Access Provider (TICAP) and the GSA Managed Trusted Internet Protocol Services (MTIPS) are based on the version 2.2 reference architecture. Understanding the capability gaps between TIC 2.2 and 3.0 is best accomplished by reviewing the updated CISA TIC Program and Use Case Guidance. To compare TIC 2.2 based TICAP and GSA MTIPS services and 3.0 security capabilities, the CISA Traditional TIC Use Case guidance should be consulted. Appendix B – Mapping TIC 2.2 Capabilities and TIC 3.0 Capabilities first outlines the TIC 2.2 capabilities and shows the mapping of the legacy capabilities, where they fit in TIC 3.0, and lists additional capabilities that were not included in version 2.2.

Enabling TIC 3.0 reference architectures and security capabilities to modernize agency networks introduces fundamental tenants of a Zero Trust Architecture (ZTA) by focusing on the security patterns of how data is accessed rather than focusing on a centralized standard security perimeter where all data access must traverse. TIC 3.0 allows the agency to decide where to apply their policy enforcement points based on data location and how it is to be best accessed for optimal user experience. Moving policy

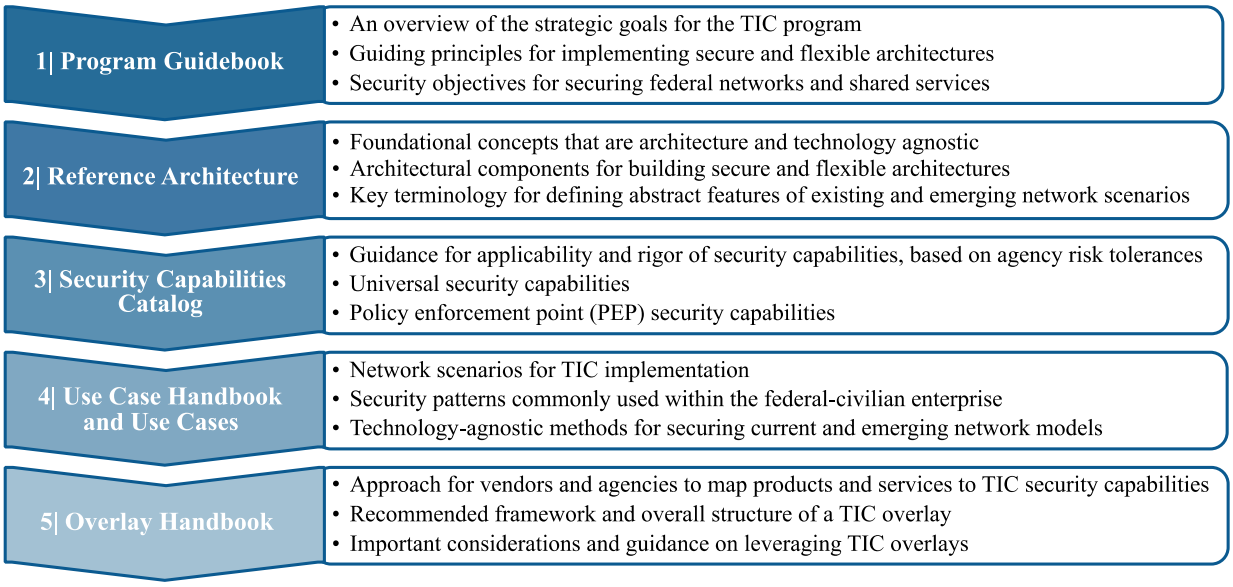
enforcement points closer to the data access areas or edges of the infrastructure is a significant component of a Zero Trust Architecture.

The following two Sections provide TIC 3.0 background and are followed by a description of recently added EIS services with guidance on how agencies can acquire services to further their infrastructure modernization goals, including the shift to SD-WAN, TIC 3.0, and eventual move to a Zero Trust Architecture.

2.0 CISA TIC Program Guidance

CISA has published updated TIC Program Guidance to support the change to TIC 3.0. The core guidance documents (Volumes 1 – 5) are final and have been posted on CISA's Trusted Internet Connections public site. The documents are structured to be read in sequential order and should be read by all Federal IT leaders, team members, and by our industry partners to better understand TIC 3.0 and how the policy compliments Federal IT Modernization.

- Program Guidebook (Volume 1)
- Reference Architecture (Volume 2)
- Security Capabilities Catalog (Volume 3)
- Use Case Handbook (Volume 4)
- Overlay Handbook (Volume 5)
- Pilot Process Handbook



3.0 CISA TIC 3.0 Use Case Guidance

In OMB M-19-26 Appendix A, the following initial common Trusted Internet Connections (TIC) Use Cases were mentioned:

1. Traditional TIC (Default Use Case): For instances not covered in other DHS TIC Use Cases, agencies are required to continue following the Traditional TIC use case. This default use case leverages agency TICAP and MTIPS providers.
2. Cloud: These sets of TIC Use Cases cover some of the most prevalent cloud models used by agencies today.
    a. Infrastructure as a Service (IaaS)
    b. Software as a Service (SaaS)
    c. Email as a Service (EaaS)
    d. Platform as a Service (PaaS)
3. Agency Branch Office: This use case assumes that there is a branch office of an agency, separate from the agency headquarters (HQ), which utilizes HQ for the majority of their services (including generic web traffic). This use case supports agencies that want to enable Software-Defined Wide Area Network (SD-WAN) technologies.
4. Remote Users: This use case is an evolution of the original FedRAMP TIC Overlay (FTO) activities. This use case demonstrates how a remote user connects to the agency's traditional network, cloud, and the Internet using government furnished equipment (GFE).

CISA has created TIC use cases to provide guidance for the secure implementation and 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 policy enforcement points (PEPs) and to describe the implementation of the security capabilities in a given scenario.

TIC use cases build upon the key concepts and conceptual implementation of TIC 3.0 presented in the TIC 3.0 Reference Architecture (Volume 2) and provides implementation guidance for applicable security capabilities defined in the TIC 3.0 Security Capabilities Catalog (Volume 3). The TIC 3.0 Use Case Handbook (Volume 4) provides general guidance for how agencies can use and combine use cases.

Agencies have flexibility in implementing TIC use cases. In particular:

- An agency may combine one or more use cases to best design and implement their TIC architectures.

- Use cases may provide more than one option for implementing a security pattern in order to give agencies flexibility.
- Each trust zone in a use case will be labeled with a high, medium, or low trust level, based on a pilot implementation or best practice. Agencies can modify this trust zone designation to meet their needs. Refer to the Reference Architecture (Volume 2) for more details on trust zones.

- When securing trust zones, agencies should consider unique data sensitivity criteria and the impact of compromise to agency data stored in trust zones. Agencies may apply additional security capabilities that have not been included in the use case.
- Agencies have the discretion to determine the level of rigor necessary for applying security capabilities in use cases, based on federal guidelines and their risk tolerance.

Refer to the Use Case Handbook (Volume 4) for more information on TIC use cases.

CISA has published the following TIC 3.0 Use Case guidance documents to assist agencies and our industry partners with an understanding of how the TIC 3.0 capabilities and security patterns apply to the given architecture. In each use case CISA offers a conceptual architecture and various security patterns in diagram and written form to describe how a given scenario can be constructed to meet the TIC 3.0 guidance.

Agencies with traditional TICAP and GSA MTIPS TIC 2.2 implementations are advised to review the Traditional TIC Use Case. Agencies who have implemented or who are implementing a SD-WAN architecture are advised to review the Branch Office Use Case. All agencies supporting remote workers are advised to review the Remote User Use Case.

- Traditional TIC Use Case
- Branch Office Use Case
- Draft TIC 3.0 Remote User Use Case

TIC Use Case Guidance planned for future releases:

- Infrastructure-as-a-Service

- Software-as-a-Service
- Platform-as-a-Service
- Email-as-a-Service

Supporting Guidance:

- IPv6 Considerations for TIC

Potential future Use Cases:

- Zero Trust
- Internet of Things (IoT)
- Partner Networks
- GSA Enterprise Infrastructure Solutions (EIS)
- Unified Communications

4.0 EIS and TIC 3.0

To assist GSA's Enterprise Infrastructure Solutions (EIS) agency customers with TIC 3.0, GSA added the Managed Security Service (MSS) Trusted Internet Connections Service (TICS) to the EIS contract to provide a flexible service where the EIS industry partners can construct and implement new TIC 3.0 solutions. MSS TICS may also be leveraged to address the TIC 3.0 security capability gaps between the current traditional TIC 2.2 services like the GSA Managed Trusted Internet Protocol Services (MTIPS) and other legacy TIC Access Provider (TICAP) implementations.

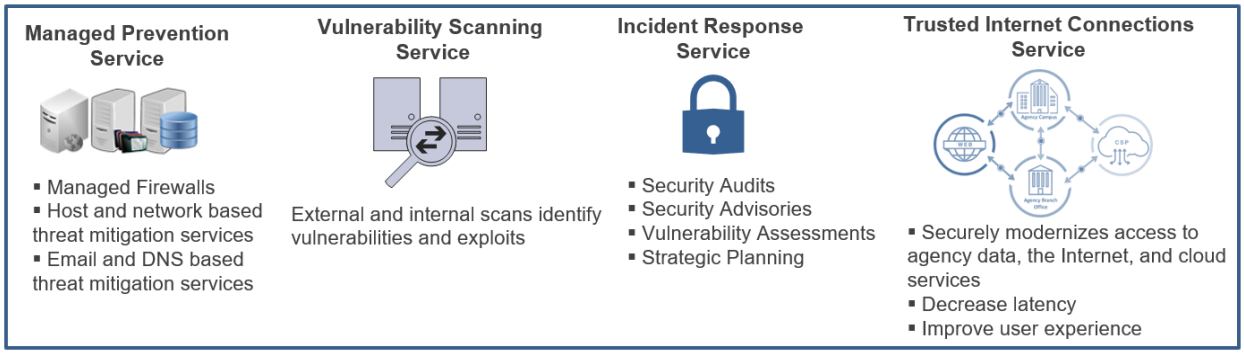
MSS TICS solutions for the Cloud, Agency Branch Office, and Remote Users Initial Common TIC Use Cases listed in OMB M-19-26 may be constructed in a number of ways under EIS. Leveraging MSS TICS, in conjunction with the SDWANS, MSS, MNS, SaaS, BIS, and other EIS services will produce a safe, flexible, and repeatable solution for the agency while meeting the CISA TIC 3.0 security objectives listed below.

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

Leveraging the Managed Security Service (MSS) and its various subservices may also lead an agency toward a Security or SOC-as-a-Service (SECaaS) arrangement with their EIS industry partner. Several EIS partners are ready to offer SECaaS now as a consumable service and are actively seeking agency requirements. Implementation of a Managed Security Services or SECaaS arrangement can significantly lower network and security management costs with centralized control and orchestration.

The four Managed Security Service (MSS) subservices are listed in the figure below. For more information on the Managed Security Service and the subservices (Managed Prevention Service, Vulnerability Scanning Service, Incident Response Service), please consult the MSS EIS Service Guide.



The MSS Trusted Internet Connections Service (TICS) within the EIS contract relies on the CISA TIC program guidance documents. TICS solutions provided under this service are to adhere to the CISA guidance.

With TIC 2.2 solutions, policy compliance was monitored for by CISA and GSA. Under TIC 3.0 neither GSA nor CISA will be issuing formal authorization stating a TIC 3.0 solution is compliant with OMB M-19-26 and the CISA TIC program guidance. TIC 3.0 is non-prescriptive cybersecurity guidance developed to provide agencies with the flexibility to secure distinctive computing scenarios in accordance with their unique risk tolerance levels. While the modernized guidance requires agencies to comply with all applicable telemetry requirements including National Cybersecurity Protection System

(NCPS) and Continuous Diagnosis and Mitigation (CDM), TIC 3.0 currently only requires agencies to self-attest on their adherence to the TIC guidance.

TICS solutions leveraged by an agency are to follow and comply with the customer agency specific Assessment and Authorization (A&A) processes while adhering to the CISA program guidance and other required National Policy Requirements. This is a major shift for the TIC program but is in line with how agencies currently authorize their other systems of record. While the TIC policy update provides greater flexibility, agencies will have to carefully consider the risks associated with hosting agency information and applications in the cloud and permitting more direct access to data.

When an EIS industry partner is proposing to meet the agency requirements for a Traditional TIC 3.0 use case, MTIPS based on the previous TIC 2.2 guidance may be proposed in combination with other Managed Security Services (MSS), Software as a Service (SaaS), Managed Network Services (MNS), Software Defined Wide Area Network Service (SDWANS), or other EIS services to fill in any security capability gaps between a TIC 2.2 and a TIC 3.0 Traditional TIC solution. The GSA MTIPS service will continue to carry the GSA ATO with the configuration of the service continuing to be based on the standardized TIC 2.2 framework and capabilities. Agencies seeking native TIC 3.0 solutions are encouraged to either place their agency requirements under the MSS TICS service (and other EIS services, as needed), or to request MTIPS plus additional MSS TIC Services to fill any capability gaps.

4.1 Technical Capabilities of MSS TICS in the EIS contract

EIS providers must meet or exceed the following Technical Capabilities when proposing MSS Trusted Internet Connections Service (TICS) solutions. (These are also listed in Section C.2.8.5.1.4 of the EIS contract.)

1. The contractor shall provide TICS solutions that adhere to the current DHS CISA Trusted Internet Connections (TIC) guidance.
2. The contractor shall ensure their TICS solutions adhere to the Key Concepts of TIC 3.0 and the Conceptual Implementation of TIC 3.0 listed in the CISA Trusted Internet Connection Reference Architecture (Volume 2) guidance.
3. The contractor shall ensure their TICS solutions contain the required Security Objectives and Security Capabilities listed in the CISA Trusted Internet Connections Security Capabilities Catalog (Volume 3) guidance.
    a. TICS solutions shall include the defined Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.

   b. TICS solutions shall include the defined Policy Enforcement Point Security Capabilities: Network-level capabilities that inform technical implementation for relevant TIC use cases.
4. The contractor shall reference the CISA TIC Use Case Handbook (Volume 4) TIC 3.0 Use Case Structure when designing and providing a TICS solution to the EIS customer. The Use Case Handbook outlines alternative security controls, such as endpoint and user-based policy enforcement point protections, that must be in place for specific instances where traffic is not required to flow through a traditional TIC 2.2 access point (i.e., TICAP or MTIPS).
5. The contractor shall reference the CISA TIC Overlay Handbook (Volume 5) guidance when constructing and proposing TICS solutions for the ordering agency customer. The Overlay Structure is a high-level mapping of a contractor's proposed TICS solution to the list of deployable security controls, security capabilities, and best practices within the Security Capabilities Catalog (Volume 3) of the CISA TIC Core Guidance. The Overlay will assist agency customers with identifying any gaps in the proposed TICS solution as it maps to the Security Objectives and Security Capabilities from the CISA TIC Core and Use Case Guidance documentation. Some proposed TICS solutions may not align with all the recommended TIC security capabilities for the intended use case, and agencies may need to obtain additional Managed Security Services from the EIS provider or other third-party providers to secure their environments to the use case specifications and their agency specific requirements.
6. The contractor proposed TICS solutions shall integrate with and support the CISA NCPS and CDM program requirements as required by the agency customer. Consult the NCPS Program and CDM Program references for further details.

In addition to the Technical Capabilities, please also review the Features and Performance Metrics in Section C (Statement of Work) of the EIS contract, and the EIS Service Guide for more information on the MSS TIC Service.

Agencies are encouraged to include any specific requirements (capabilities, features, and performance metrics) that are in addition to what is included in the base contract for any EIS service. Doing so ensures that the industry partners have a clear understanding of what the agency expectations are for a specific service or solution set.

4.2 How to obtain TIC 3.0 capable solutions

Agencies may add requirements to their GSA Enterprise Infrastructure Solutions (EIS) solicitation to include requirements for the Managed Security Service along with specific

Trusted Internet Connections and other Security Services requirements. The MSS TIC Service (TICS) requirements in the EIS contract lean heavily on the CISA TIC guidance. The EIS industry partners shall ensure their proposed solutions map to agency's needs using the CISA Overlay Handbook (Volume 5) template to demonstrate how they meet (or do not meet) the TIC 3.0 requirements of a specific use case or set of requirements. The overlay will also illustrate how the proposed solution is in line with CISA's guidance. There may be cases where an industry partner's solution does not map to all of the TIC 3.0 capabilities. The industry partner may propose other EIS services, such as Service Related Equipment (SRE) and Service Related Labor (SRL), to fill the gaps.

When soliciting for MSS TICS solution sets to adopt TIC 3.0 or other modern network security architectures, remaining open to alternative solutions being proposed by the industry partners may help the agency move their IT modernization planning and goals forward sooner. Specifying any agency-specific requirements is still encouraged when asking for an alternative solution leveraging a Statement of Objectives (SOO) approach. EIS providers should incorporate any agency-specific performance metrics, capabilities, and features, as applicable, when proposing any alternate approaches.

Agencies are encouraged to add requirements in their solicitation for the EIS industry partner to assist with the Assessment and Authorization preparations to obtain the agency's Authority to Operate (ATO). The EIS industry partners are ready to assist agencies with this task leveraging Service Related Labor under the Managed Security Service.

GSA contracts such as the Multiple Award Schedule (MAS) and Government Wide Acquisition Contracts (GWACs) may also enable the transition and support of integrated or managed TIC 3.0 solutions.

GSA can assist Agencies with:

- Solicitation Templates for WAN Modernization
- Scope Reviews of Solicitations
- Technical Consultation to help plan an agency's TIC 3.0 journey
- Service Provider Coordination and Contract Support

4.3 EIS MSS TICS Ordering and Pricing Information

The Managed Security Service (MSS) and its four subservices follow the EIS Catalog Pricing Model. That is, MSS TICS CLINS are not priced on the EIS master contract. Although pricing occurs at the agency order-level, the catalog approach encourages repeatability and commonality were feasible.

More information on the pricing of MSS can be found in Section B of the EIS contract. The following information is contained in Section B.2.8.5.

Where MSS offerings include equipment, all MSS-related equipment or equipment features shall be identified and priced in accordance with the SRE requirements in Section B.2.10. Where MSS-related labor is offered, then labor rates shall be specified and priced in accordance with Section B.2.11.

Otherwise, MSS prices for non-labor and non-SRE elements shall be determined from the catalog based on the information required as shown in Table B.2.8.5.2 below. Charging mechanisms are defined in Table B.2.8.5.5. Additional discounts or reduced prices may be negotiated at time of TO award between the ordering agency and the contractor.

The contractor shall assign each item in MSS Catalog Table B.2.8.5.2 to one or more of the MSS categories listed in Reference Table B.2.8.5.4. Additional MSS categories may be defined upon request by the contractor.

Task Order Unique CLINs (TUCs) shall be used as defined in Section B.1.2.15.

5.0 Recommendations

- Review the CISA TIC 3.0 Program and Use Case Guidance
- Review the TIC 3.0 Remote User Use case, consider your remote access traffic patterns, and perform an assessment on split tunneling to enable more direct to cloud access for productivity applications like Microsoft 365 and Google Workspace
- Consider implementing SD-WAN and the TIC 3.0 Branch Office Use Case to increase user experience while potentially reducing costs
- Review your current Identity Access Management, Endpoint Security Management and Remote Access services to identify where best to implement principles of the TIC 3.0 use cases while also supporting your shift to a Zero Trust Architecture (ZTA). The TIC 3.0 use cases are fundamental components and enablers of a Zero Trust Architecture.
- Consider a Managed or Co-managed solution using the EIS MSS and/or MNS services
- Increase available bandwidth with the Broadband Internet Service (BIS) and Wireless Service (MWS)
- Reach out to your GSA Solutions Broker to engage GSA resources for assistance with reviews of your current architecture to identify areas for

modernization, and for solicitation advice leveraging GSA EIS tools, products, and services.

Contact your designated GSA representative at https://gsa.gov/nspsupport or call 855-482-4348