Use Case Highlights

Zero Trust Architecture (ZTA) is a security concept or approach based on “trust no one always verify” and is a fundamental switch from perimeter-based security models. Instead of trusting users and devices that are verified at the perimeter of the network, no one can be trusted until verified; with an additional layer of security for access to systems and applications. Additionally, behaviors can be monitored to ensure ongoing trustworthiness.

The ZTA covers five pillars: Identity, Devices, Networks, Applications & Workloads, and Data; and three cross-cutting capabilities: Visibility & Analytics, Automation and Orchestration, and Governance. Zero Trust Guidance is available in the Cybersecurity and Infrastructure Security Agency (CISA) Trusted Internet Connections (TIC) 3.0 Core Guidance and Cloud Security Technical Reference Architecture documents as well as the publications listed under the Enterprise Infrastructure Solutions (EIS) ZTA solutions sets below. GSA's EIS industry partners can help agencies with the planning and implementation of their ZTA solutions in alignment with the goals of Executive Order 14028, Improving the Nation’s Cybersecurity [Sec. 3 (a – c)].

EIS ZTA solution sets are consistent with:

- The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 description of ZTA.
- The CISA Zero Trust Maturity Model (ZTMM) Version 2; adds clarity to continued modernization within evolving environments.
- Office of Management and Budget (OMB) Memorandum M-19-26, “Update to Trusted Internet Connections (TIC) Initiative.”

EIS is an ideal contract vehicle to plan, implement, and operationally support the logical components of your ZTA deployment.

How to Get It

ZTA is not a service that you purchase but a concept that you implement through the services that you purchase. EIS services such as the Software-Defined Wide Area Network Service (SDWANS), Managed Security Services (MSS), Managed Network Services (MNS), Managed Mobility Services (MMS), and the cloud services (IaaS, PaaS, SaaS) can provide the logical components and ongoing operational support of a ZTA. GSA also has a white paper regarding **Zero Trust** if more information is needed.

Other GSA contracts, such as the Multiple Award Schedule (MAS) and Governmentwide Acquisition Contracts (GWACs), can also support integrated or managed ZTA solutions.

GSA published the “**Zero Trust Architecture (ZTA) Buyer’s Guide**” to help agencies.

- The tenants of a ZTA as noted in NIST SP 800-207 are instrumental in identifying and managing

Business Value

cybersecurity risks.

- Implementing a ZTA will help agencies access the benefits of cloud computing and shared services while increasing security and potentially lowering overall costs.
- Implementing elements of a ZTA will improve user experiences by enabling direct access to the internet and to cloud resources while optimizing data-access traffic patterns and preventing bottlenecks.
- EIS industry partners can directly help with agency planning, implementation, and continued operational support of the logical components of a ZTA solution by leveraging EIS managed service offerings.
- Software-Defined Wide Area Networking (SD-WAN) pricing models indicate significantly lower total cost of network management with centralized control and orchestration.

Recommendations

- Agencies should implement ZTA as part of their comprehensive modernization and virtualization strategy integrated with other components such as SD-WAN, TIC 3.0, and Internet Protocol version 6 (IPv6). The Agency's security posture and risk tolerance should be factored into the overall ZTA approach.

- Reach out to your GSA Solutions Broker to engage GSA resources for help with reviews of your current architecture to identify areas for modernization – and for solicitation advice to leverage GSA tools, products, and services.
- Review the CISA Zero Trust Maturity Model v2.0 and the NIST SP 800-207 description of ZTA.
- Ensure the solutions address CISA's five distinct ZTA pillars: Identity, Devices, Networks, Applications & Workloads, and Data. Factor plans against current maturity level: Traditional, initial, advanced, and optimal.
- Agencies should reference CISA's Program Guidebook, Reference Architecture, Security Capabilities Catalog, Use Case Handbook, and Overlay Handbook to determine how to protect their environments and comply with their risk management strategy and the security considerations outlined in TIC use cases.

EIS Services Enabling ZTA

The following EIS services may be combined to obtain components of Zero Trust Architecture solution sets.

Software-Defined Wide Area Network Service (SDWANS) – Implement managed or co-managed SD-WANS as an "overlay" to better enable the logical components of a ZTA and several of the TIC 3.0 Use Cases. Multiple "underlay" transport and access (e.g., Internet Protocol Service [IPS], broadband internet, mobile wireless) can be utilized for increased availability.

Managed Security Services (MSS) – Comprehensive cybersecurity solutions such as Cloud Access Security Brokers (CASB), Identity and Access Management, Endpoint Management, Secure Web Gateway, and Trusted Internet Connections (TIC).

Managed Network Services (MNS) – Network planning, design, implementation, maintenance, operations, and customer service.

Cloud Services – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are FedRAMP-authorized cloud-based solutions.

Managed Mobility Services (MSS) – Manage mobile devices, wireless networks, and other mobile computing services.

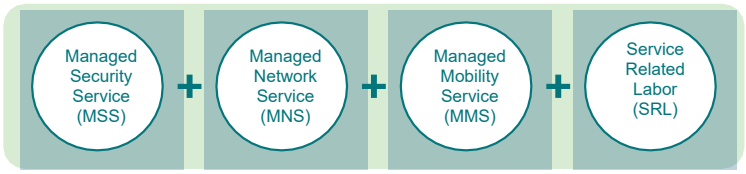
Service Related Equipment (SRE) – Equipment required to fully deploy an EIS service.

Service Related Labor (SRL) – EIS network services already include all SRL necessary to implement the services. However, in a task order for procuring one or more network services, an agency may opt to include additional labor to support the EIS services.

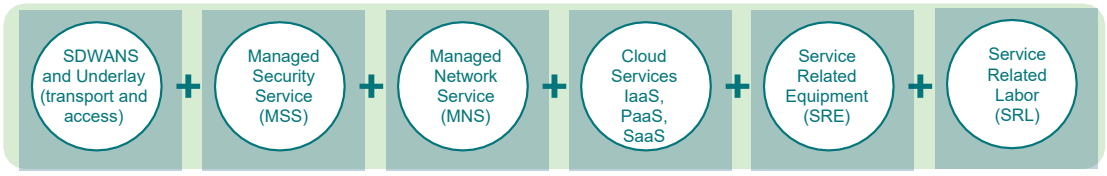
EIS Services Enabling ZTA

Examples of how EIS services may be combined to support ZTA components.

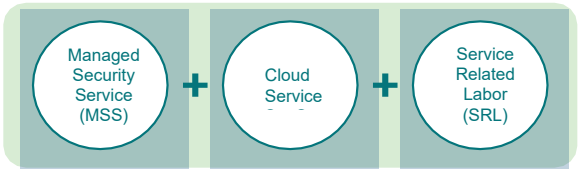
Example 1 – TIC 3.0 Branch Office, Remote User, and or Cloud Use Case solutions – Improve productivity and user experience for the Agency's workers with secure and optimized paths to the internet, cloud service providers, and agency internal resources.



Example 2 – Secure Access Service Edge (SASE) – a network architecture that combines VPN and SD-WAN capabilities with cloud-native security functions such as secure web gateways, cloud access security brokers, firewalls, and zero-trust network access.



Example 3 – Cloud Access Security Broker (CASB) – cloud-hosted software that acts as a policy enforcement point between users and cloud service providers.



For more information

Contact your designated GSA representative at www.gsa.gov/nspsupport or call (855) 482-4348.

Contributors

General Services Administration (GSA)
Java Productions, Inc. (JPI)