

**Zero Trust Architecture (ZTA)**

The Zero Trust Architecture (ZTA) model represents a shift in how the Federal Government will secure its infrastructure, networks, and data in comparison to the legacy perimeter-based model in which access is verified once by a single authentication, device profile interrogation, or firewall rule allowance at a defined boundary entry or exit point. The ZTA model enforces continuous verification of each user, device, or application function while ensuring that data access transactions are consistently reauthorized according to the established policies throughout the session.

**Agency Use Case Highlights**

**Remote Workforce Use Case**

* Agencies may be facing an increased demand for remote user capabilities because of the rapid expansion of the remote workforce
* Data and application access needs of remote users are largely agency campus based resources and data
* Cloud Access Security Broker (CASB) solutions permit connectivity from remote users to agency-hosted resources through a CASB or other Security-as-a-Service (SECaaS) provider(s)
* Policy enforcement can be performed at the CASB, the agency campus, and, if possible, directly on the remote user’s device. Policy enforcement parity between the agency campus and remote users, as well as other remote entities (e.g. branch offices) can be simplified when the locations use the same CASB or SECaaS provider(s)

**Advantages**

* By satisfying the remote user requirements via this combination of Enterprise Infrastructure Solutions (EIS) managed services an agency relieves the pressure on their limited Virtual Private Network (VPN) resources and will result in a better user experience by allowing more direct access to agency resources
* Access to agency applications and data is granted on the basis of user and device profiles reducing the agency’s cyber-attack surface and vulnerability as they progress further toward their ZTA goals
* Utilizing ZTA can Improve productivity and the user experience of remote workers with secure and optimized paths to the internet, Cloud service providers, and agency internal resources by implementing the Managed Mobility Services (MMS) to manage the end user devices, and Managed Network Services (MNS) and Managed Security Services (MSS) to manage access on a user and device basis to the agency resources

Rows of computer servers

Description automatically generated with medium confidence

**How to Get It**

* In June 2021, GSA published the “[Zero Trust Architecture Buyer's Guide](https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%2020210810.pdf)” to assist agencies with acquiring products and services to support and align with their Zero Trust Security StrategyA picture containing text, sign

  Description automatically generated
* EIS Managed Services, Cloud and Other Related EIS services are identified in the “ZTA Buyer’s Guide,” as well as specific GSA Multiple Award Schedule (MAS) Special Item Numbers (SINs) and Government Wide Acquisition Contracts
* The Federal Government had a significant digital transformation with the continued emphasis of mitrating mission support applications and data to Cloud computing resources, while also accommodating the expansion of the remote workforce

**Business Value**

* The traditional perimeter-based network security model is based on the concept that traffic outside of the perimeter boundary is untrusted and that the traffic inside is trusted
* The transformation and expansion of agency data access locations and system boundaries make the traditional perimeter-based cybersecurity model ineffective as perimeters no longer define the scope of where security policy enforcement must occur for agency data access. ZTA addresses these limitations and provides a more modern approach to network security

**Recommendations**

* The Federal Zero Trust Strategy requires agencies to achieve specific zero trust security goals by the end of Fiscal Year (FY) 2024. As such, Agencies should focus network security acquisitions on ZTA to successfully comply with evolving mandates
* The Office of Management and Budget (OMB) ZTA established goals that follow CISA Zero Trust Maturity Model Pillars (Identity, Devices, Networks, Applications/Workloads, and Data) and each goal has a Vision and associated action(s). The OMB memorandum M-22-09 requires agencies to have zero trust security goals by the end of Fiscal Year (FY) 2024. GSA can aid agencies with meeting the identified OBM goals through streamlined acquisitions

# 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)