



U.S. General Services Administration



Zero Trust Architecture (ZTA)

Buyer's Guide

Table of Contents

1 Executive Summary 1

2 Purpose..... 1

3 Audience..... 1

4 What is a Zero Trust Model..... 1

5 CISA and NIST ZTA Standards and Guidance 2

6 ZTA Core Components and Functions 3

6.1 Cross-Cutting Capabilities of ZTA..... 3

6.2 Pillars of ZTA..... 4

6.3 Zero Trust Maturity Stages..... 5

6.4 Logical Components of ZTA..... 6

6.5 Essential Functions 6

7 Key Considerations for ZTA Products, Services, and Solutions 9

8 ZTA Buyer’s Guide Contact Information 10

Appendix A – GSA-Offered Products, Services, and Solutions for ZTA 11

Appendix B – References..... 40

Appendix C – GSA Vehicle Reference 41

Appendix D –Zero Trust Reference Architecture 45

Table of Figures

Figure 1- ZTA Core Components and Functions 3

Figure 2- Zero Trust Reference Architecture..... 45


Foreword

This third version of the Zero Trust Architecture (ZTA) Buyer's Guide aims to assist federal agencies in acquiring products, services, and solutions that align with the Federal Zero Trust Strategy and enable the implementation of robust security measures across the critical infrastructure sectors.

Developed with the expertise of cybersecurity professionals and industry leaders, this guide provides valuable insights, best practices, and key considerations to aid federal agencies in their journey toward implementing a ZTA. By embracing the principles of Zero Trust, agencies can enhance their security posture, safeguard High-Value Assets (HVAs), and mitigate the risks posed by sophisticated cyber threats.

The General Services Administration (GSA) thanks all of the contributors and subject matter experts who have generously shared their knowledge and expertise to make this guide comprehensive and practical. GSA's Information Technology Category (ITC) is available to answer any questions and provide subject matter expertise related to any aspect of this guide and any other information technology (IT) needs.

Approval

DocuSigned by:

99B68D3F19DB4B4...

Laura Stanton
Assistant Commissioner
Information Technology Category (ITC) Federal Acquisition Service (FAS) General Services
Administration (GSA)

1 Executive Summary

The ZTA Buyer's Guide for federal agencies is a comprehensive resource designed to assist agencies in their efforts to align with the Federal Zero Trust Strategy. As cyber threats continue to evolve in complexity and sophistication, traditional perimeter-based security approaches have proven inadequate in protecting critical assets. The adoption of ZTA has emerged as a crucial strategy for enhancing cybersecurity and maintaining the integrity of federal agency networks.

This guide is meant to be leveraged as an onramp for acquiring and implementing Zero Trust products, services, and solutions, enabling them to build resilient and more secure IT environments capable of withstanding today's sophisticated cyber threats.

2 Purpose

The purpose of the ZTA Buyer's Guide is to provide federal agencies with practical guidance on acquiring products, services, and solutions that support the agency's implementation of a ZTA. It outlines the cross-cutting capabilities (also known as the foundational levels), technology pillars, logical components, and essential functions of ZTA to give GSA consumers all the knowledge they need to make an informed decision before purchasing.

By following the recommendations outlined in this guide, federal agencies can enhance their security posture, minimize risks, and enable secure access to critical resources. This guide emphasizes the importance of collaboration between agency stakeholders and industry partners to ensure successful implementation and alignment with the Federal Zero Trust Strategy.

3 Audience

The audience for this guide includes Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT managers, and security professionals who are responsible for protecting the data or critical infrastructure of a federal agency against cyber attacks.

The ZTA Buyer's Guide is suitable for any federal agency which is considering implementing a ZTA or is already in the process of doing so. It provides practical guidance on evaluating and selecting Zero Trust products, services, and solutions and best practices for implementing and maintaining a ZTA. The guide assumes a basic understanding of cybersecurity and network architecture concepts.

4 What is a Zero Trust Model

The concept of Zero Trust was present in cybersecurity before the term "Zero Trust" was coined. Zero Trust is not a technology, but a shift in approach to cybersecurity. In 2010, a Zero Trust model was architected by John Kindervag, Principal Analyst at Forrester Research, who coined the term "Zero Trust" architecture. Kindervag based the proposed architecture on the understanding that the typical "defense-in-depth" approach was flawed due to the inherited trust

model. In the Zero Trust model, all traffic is deemed hostile, and he asserted, “We needed a new model that allows us to build security into the DNA of the network itself.” Kindervag noted five (5) concepts to make ZTA actionable:

1. All resources must be accessed in a secure manner.
2. Access control is on a need-to-know basis.
3. Do not trust people, verify what they are doing.
4. Inspect all log traffic coming in on the network for malicious activity.
5. Design networks from the inside out.

Zero Trust then became the term used to describe various cybersecurity solutions that moved away from the implied trust based on network location and instead focused on evaluating trust on a per-transaction basis. Today there are various Zero Trust models, such as models developed by CISA, NIST, the National Security Agency (NSA), and the Department of Defense (DoD). For this guide, GSA followed the guidance from the Office of Management and Budget (OMB) Memorandum (M)-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, issued on 26 January 2022. GSA has also adopted a combination of CISA and NIST Zero Trust standards and guidance.

5 CISA and NIST ZTA Standards and Guidance

The *CISA Zero Trust Maturity Model (ZTMM)*, Version 2.0, dated April 2023; and NIST SP 800-207 are two complementary frameworks that work together to guide organizations in implementing effective Zero Trust strategies. The CISA ZTMM provides a maturity-based approach for organizations to assess their current Zero Trust capabilities, identify gaps, and gauge progress toward higher levels of maturity. It helps organizations understand the key components of Zero Trust and provides a roadmap for incremental improvements.

The NIST SP 800-207 complements the CISA ZTMM by providing detailed guidance on the principles, concepts, and components of a ZTA. It outlines the core tenets of Zero Trust, such as continuous verification, least privilege access, micro-segmentation, and provides recommendations for their implementation. It serves as a comprehensive resource to help organizations design, deploy, and operate a ZTA.

When used together, these frameworks complement each other by providing a holistic approach to Zero Trust implementation. The CISA ZTMM helps organizations assess their current maturity level and identify areas for improvement, while NIST SP 800-207 offers guidance and best practices for implementing the various components of a Zero Trust Architecture. Organizations can leverage the maturity model to gauge their progress and track their advancements while following the NIST ZTA guidelines to ensure robust and effective implementation.

By aligning with both the CISA ZTMM and NIST SP 800-207, agencies can establish a strong foundation for their Zero Trust initiatives. They can systematically evaluate their capabilities, implement appropriate controls and technologies, and continuously enhance their security posture to effectively combat evolving cyber threats. The integration of these frameworks enables agencies to adopt a risk-based approach and tailor their Zero Trust implementation according to their specific needs and organizational context, ultimately achieving a resilient and secure IT environment.

6 ZTA Core Components and Functions

The proponents of Zero Trust Architecture emphasize it is a paradigm, not a technology. Each organization may implement Zero Trust in different ways. The core components which include the cross-cutting capabilities, technology pillars, logical components, and essential functions are shown in Figure 1 below.

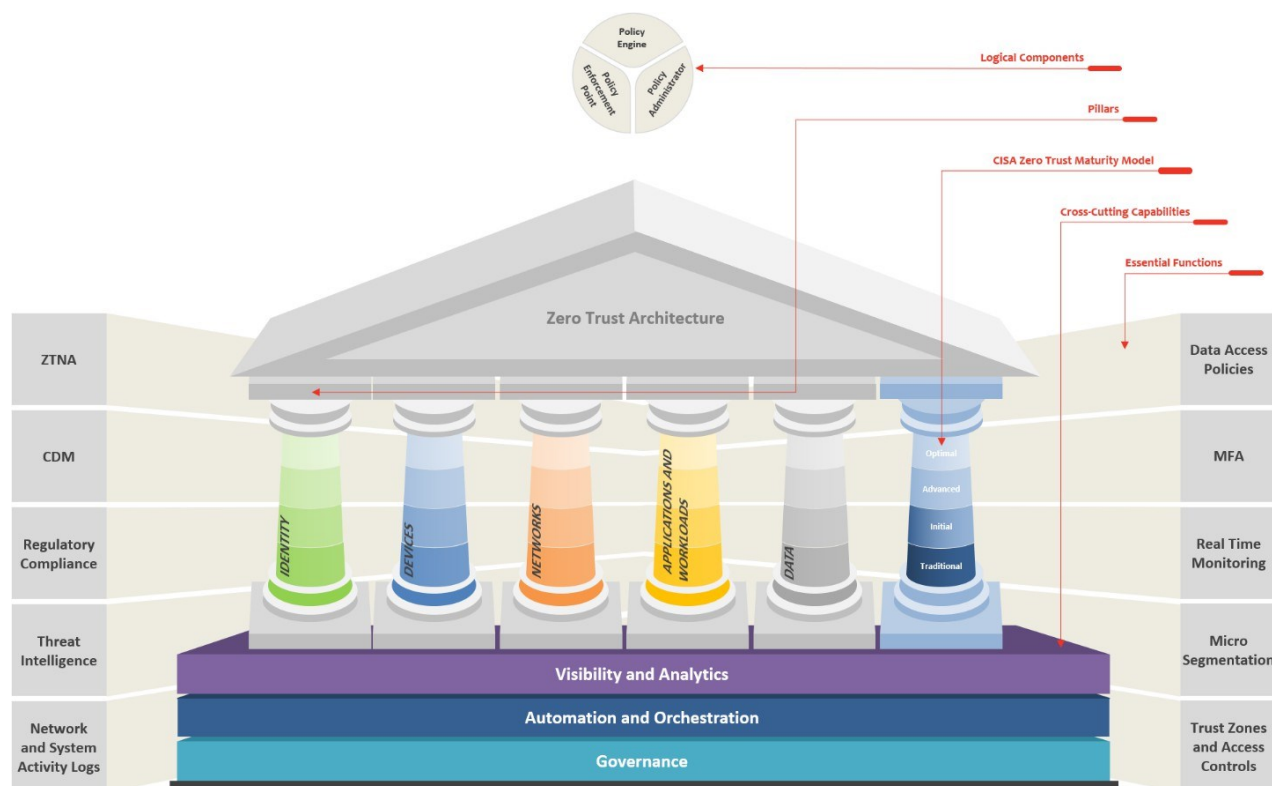


Figure 1- ZTA Core Components and Functions

6.1 Cross-Cutting Capabilities of ZTA

Each ZTA pillar includes general details regarding the following three (3) cross-cutting capabilities to support integration with the pillar and across the model: Governance, Automation and Orchestration, and Visibility and Analytics. Each cross-cutting capability is described below.

1. **Governance:** Governance refers to the definition and associated enforcement of agency cybersecurity policies, procedures, and processes, within and across pillars, to manage an agency's enterprise-wide environment and mitigate security risks in support of Zero Trust principles and fulfillment of federal requirements.
2. **Automation and Orchestration:** Zero Trust makes full use of automated tools and workflows that support security response functions across products and services while maintaining oversight, security, and interaction of the development process for such functions, products, and services.
3. **Visibility and Analytics:** Visibility refers to the observable artifacts that result from the characteristics of events within enterprise-wide environments. The focus on cyber-related data analysis can help inform policy decisions, facilitate response activities, and build a risk profile to develop proactive security measures before an incident occurs.

6.2 Pillars of ZTA

The five (5) pillars of the Zero Trust Maturity Model are Identity, Devices, Networks, Applications and Workloads, and Data. Each pillar is described below.

1. **Identity:** An identity refers to an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities. Users include employees, contractors, and customers. To implement Zero Trust, an agency must first have an accurate picture of who and what should actually be trusted resources. Then the agency must establish methods to securely authenticate the identity of its users.
2. **Devices:** A device refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, desktop and laptop machines, printers, mobile phones, Internet of Things (IoT) devices, networking equipment, and more. Organizations must first understand their full set of devices, then Zero Trust policies can be implemented based on the context of the device.
3. **Networks:** A network refers to an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages. Networks include all public, private, and virtual networks within an organization. Organizations must first understand their existing set of networks and segment them to prevent lateral movement. Then, Zero Trust policies can be created that granularly control the segments of a network which users and devices can access.
4. **Applications and Workloads:** Applications and workloads include agency systems, computer programs, and services that execute on-premises, on mobile

devices, and in cloud environments. Organizations must understand the applications that exist and then establish Zero Trust policies for each application or, in some cases, block unapproved applications.

5. **Data:** Data includes all structured and unstructured files and fragments that reside or have resided in federal systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and off-premises) as well as the associated metadata. Organizations must understand where their sensitive data exists. Then they can establish Zero Trust controls to block sensitive data from being accessed and exfiltrated.

When evaluating a solution that aligns with an agency's planned deployment of a ZTA, agencies should consider how well the product or service addresses the five (5) pillars and to what extent.

The CISA Zero Trust Maturity Stages in the next section provides a gradient of implementation across the five (5) distinct pillars to facilitate implementation, allowing agencies to make minor advancements over time toward the optimization of Zero Trust Architecture.

6.3 Zero Trust Maturity Stages

The Zero Trust maturity stages are used to identify maturity for each Zero Trust technology pillar and provide consistency across the maturity model. The guiding criteria for each of the four (4) stages of maturity are detailed below.

1. **Traditional:** Manually configured life cycles (i.e., from the establishment to decommissioning) and assignments of attributes (security and logging); static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry.
2. **Initial:** Starting automation of attribute assignment and configuration of life cycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
3. **Advanced:** Wherever applicable, automated controls for life cycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to predefined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources).
4. **Optimal:** Fully automated, just-in-time life cycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated/observed triggers; dynamic least privilege access (just enough and within thresholds) for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous

monitoring; and centralized visibility with comprehensive situational awareness.

6.4 Logical Components of ZTA

The NIST SP 800-207 describes the functionality of three (3) logical components to establish and maintain a ZTA. The components are described below.

- 1. Policy Engine (PE):** PE is the core component to implement the capability of continuous trust evaluation in a ZTA. The PE is linked with the Policy Administrator (PA) to provide trust level assessment for authorization decisions. The PE combines behavioral analytics, external threat intelligence, enterprise security policy, regulatory requirements, and identity and authority baselines to evaluate and generate access decisions (grant, deny or revoke access). While the PE makes and logs the access decision, it is the PA that enforces this decision.
- 2. Policy Administrator:** The PA is responsible for establishing and/or shutting down the communication path between a subject and a resource via commands to relevant Policy Enforcement Points (PEPs). The PA component is linked to the PEP to authenticate and dynamically authorize all access requests based on policy decisions by the PE. The authorization is based on context attributes, trust levels, and security strategies. If the session is authorized and the request authenticated, the PA signals the PEP to allow the session to start. Otherwise, the session is denied, and the PA directs the PEP to shut down the connection.
- 3. Policy Enforcement Point:** The PEP is a data plane component. It is the gateway to secure access to government resources, where the adaptive access control capability is enforced. After the PEP intercepts the access request, the requestor is authenticated through the PA, and authority is determined dynamically. Only access requests that are authenticated and authorized are deemed trustworthy and allowed to gain access to government resources.

6.5 Essential Functions

For the PE to reach an access decision, the input of data from various sources is required. Although these sources are not the core components of a ZTA, they are essential to the effectiveness and efficiency of Zero Trust. These can include, but are not limited to:

- **Zero Trust Network Access (ZTNA):** A ZTNA solution is designed to implement and enforce a Zero Trust strategy across the enterprise network. Users attempting to connect to an organization's systems and applications are only allowed to connect if they specifically need access to perform their roles.

ZTNA can take several forms:

- **Gateway Integration:** ZTNA functionality can be implemented as part of a network gateway. Traffic crossing network boundaries is filtered by the gateway according to the defined access control policies.

- **Software-Defined Wide Area Network (SD-WAN):** SD-WAN optimizes networking across an enterprise WAN. Secure SD-WAN solutions integrate a full security stack into the network infrastructure, and this can include ZTNA functionality. SD-WAN with built-in ZTNA can provide sophisticated, centralized access control.
- **Secure Access Service Edge (SASE):** SASE is a broad solution that includes a secure web gateway (SWG), Firewall as a Service (FWaaS), a cloud security access broker (CASB), and ZTNA. SASE provides a holistic solution to enterprise networking, which strongly supports the Zero Trust model.
- **Continuous Diagnostics and Mitigation (CDM):** CDM is a systematic approach that involves real-time monitoring of an organization's IT infrastructure, assets, and users. It continuously collects data on system configurations, vulnerabilities, and user activities. This data is then analyzed to identify potential security issues and compliance violations. CDM provides organizations with a constant stream of information about their security posture, helping them make informed decisions about risk management and security remediation. The integration of Continuous Diagnostics and Mitigation with a Zero Trust Architecture creates a powerful cybersecurity framework that continuously monitors, assesses, and enforces security policies, helping organizations adapt to evolving threats and enhance their overall security posture.
- **Regulatory Compliance:** Ensures the compliance of agency policies with regulatory security requirements. Such regulations include the Federal Information Security Modernization Act (FISMA); Federal Risk and Authorization Management Program (FedRAMP); Federal Identity, Credential, and Access Management (FICAM); Homeland Security Presidential Directive 12 (HSPD-12); General Data Protection Regulation (GDPR); and others as applicable.
- **Threat Intelligence:** Provides information from internal or external sources about newly discovered attacks or vulnerabilities that help the PE make dynamic and adaptive access decisions.
- **Network and System Activity Logs:** Aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.
- **Data Access Policies:** They define the attributes, rules, and policies for access to enterprise resources. The policies form the foundation for authorizing access to a resource as they provide the basic access privileges for accounts and applications/services in the enterprise. These policies should be mission tailored to accommodate organizational needs.

- **Multifactor Authentication:** MFA is the use of multiple methods to verify user identity before granting access. These checks may include security questions, email verification, text messages, security tokens, biometric identification (ID) checks, and more. Implementing MFA at every access point both for ingress traffic flowing into the network and for connections within the network is a foundation of Zero Trust.
 - **Enterprise Public Key Infrastructure (PKI):** This system is responsible for managing the life cycle of digital certificates (X.509) issued by the enterprise to resources, subjects, services, and applications.
 - **Identity, Credential, and Access Management (ICAM):** This system is responsible for creating, storing, and managing both enterprise user accounts and identity records and federated non-enterprise, partner accounts. It contains the necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets.
- **Real-Time Monitoring:** Real-time monitoring continuously evaluates the network to detect intruders and limit damage if internal systems are compromised. Effective monitoring can reduce “breakthrough time,” which is the amount of time a hacker needs to move laterally or escalate privileges, after initially penetrating an application or device. Zero Trust monitoring strategies must include automated components, typically based on behavioral profiling and anomaly detection, and rapid triage and response of incidents by security analysts.
 - **Security Information and Event Management (SIEM):** This technology solution collects security-centric information for later analysis to refine policies and warn of possible attacks against enterprise assets.
- **Micro-segmentation:** Another important aspect of Zero Trust is network micro-segmentation. Micro-segmentation is the ability to create isolated perimeters within the network, allowing connections within each perimeter, but blocking access between them. This means that once a user or entity is authorized to access the network, they are limited to a specific, isolated space and resource, with limited ability to move laterally and access other systems. A crucial aspect of micro-segmentation is that it is automated and centrally controlled by the Zero Trust solution. Zero Trust technology must be able to adjust micro-segmentation dynamically in response to changing security policies and current security conditions.
- **Trust Zones and Default Access Controls:** Trusted Internet Connection (TIC) 3.0 is the latest version of an initiative by the U.S. Government aimed at standardizing management of external network connections. TIC enables an organization to divide the network into trusted zones, allowing users to share data within zones, with centrally defined default access controls but prohibiting access between zones. Trust zones can only be used if all

network traffic is encrypted and access to all systems is centrally controlled using a Zero Trust solution.

- **Data and Analytics:** Data and analytics constitute an essential component within the ZTA, serving as the intelligence backbone that fuels the ZTA's core principles. Data analytics continuously scrutinizes user and device behavior, network traffic patterns, and application interactions, facilitating real-time risk assessment and anomaly detection. This contextual insight enables ZTA to enforce granular access controls, allowing access only to trusted entities based on verifiable data points like identity, location, and behavior. Furthermore, advanced analytics, including machine learning, bolster threat detection capabilities, swiftly identifying security incidents or breaches. By employing data and analytics, ZTA elevates security postures, fostering adaptive and dynamic protection against evolving threats while improving overall network visibility, compliance, and incident response.

7 Key Considerations for ZTA Products, Services, and Solutions

When acquiring products, services, and solutions to support and align with the Federal Zero Trust strategy, federal agencies should carefully evaluate a range of factors to ensure they meet their specific requirements. The following key considerations will help agencies make informed decisions and select the most suitable ZTA products, services, and solutions:

1. **Alignment with Zero Trust Principles:** Ensure the product, service, or solution aligns with the core principles of Zero Trust, including the principle of “never trust, always verify.” It should provide granular access control, strong authentication mechanisms, continuous monitoring, and least privilege access.
2. **Interoperability and Integration:** Assess the ability of the product, service, or solution to seamlessly integrate with existing IT infrastructure and security tools. Compatibility and interoperability are crucial to avoid disruptions, simplify deployment, and enable consistent enforcement of security policies across the network.
3. **Scalability and Flexibility:** Consider the scalability and flexibility of the solution to accommodate evolving business needs and future growth. It should be able to handle increasing workloads, adapt to changing technologies, and support a diverse range of devices, platforms, and applications.
4. **Comprehensive Threat Protection:** Evaluate the solution's capabilities for threat detection, prevention, and response. The solution should provide advanced threat intelligence, behavior analytics, and real-time monitoring to detect and mitigate potential security breaches. Federal agencies should also look for features such as network segmentation, encryption, and anomaly detection to enhance protection.
5. **User Experience:** Consider the impact of the solution on user experience and productivity. The solution should provide seamless access to authorized users while minimizing friction.

and unnecessary authentication steps. User-friendly interfaces, self-service capabilities, and efficient identity and access management processes contribute to a positive user experience.

- 6. Compliance and Regulatory Requirements:** Ensure the solution meets the compliance and regulatory requirements specific to federal agencies. Consider frameworks such as NIST SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*; FISMA; and FedRAMP to ensure adherence to industry standards and best practices.
- 7. Vendor Expertise and Support:** Evaluate the vendor's expertise, reputation, and record of accomplishment in delivering Zero Trust solutions. Consider its ability to provide ongoing support, updates, and timely responses to security vulnerabilities or emerging threats.
- 8. Cost and Return on Investment:** Assess the total cost of ownership, including upfront costs, licensing fees, ongoing maintenance, and operational expenses. Consider the potential return on investment in terms of improved security, reduced risk, operational efficiency gains, and long-term sustainability.
- 9. Training and Documentation:** Evaluate the availability of comprehensive training materials, documentation, and user guides to facilitate implementation, configuration, and ongoing management of the solution. Adequate training and support contribute to the successful adoption and utilization of the Zero Trust Architecture.
- 10. Futureproofing:** Consider the solution's roadmap and vendor commitment to innovation, continuous improvement, and addressing emerging security challenges. Ensure the chosen solution can evolve alongside evolving threats and technological advancements.

Federal agencies should consider these key factors when selecting ZTA products, services, and solutions to best meet their unique needs, align with the federal Zero Trust strategy, and enhance their overall security posture.

8 ZTA Buyer's Guide Contact Information

For questions related to any aspect of this guide, or ZTA products, services, or solutions, contact:

- E-mail ITSecurityCM@gsa.gov for Customer Support with the ZTA Buyer's Guide.
- E-mail RMASS@gsa.gov for any ZTA Buyer's Guide comments, suggestions, and options.
- Contact the respective acquisition support for the GSA Schedules identified in Appendix A of this ZTA Buyer's Guide.

Appendix A – GSA-Offered Products, Services, and Solutions for ZTA

The below table lists GSA Schedules to obtain ZTA-related products, services, and solutions.

Table 1 - ZTA Buyer's Guide-Offered Products, Services, and Solutions

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Identity	User Inventory	<p>A complete account of every user account across the varied systems of an organization.</p> <ul style="list-style-type: none"> User accounts are generally associated with a wide range of platforms — from databases to applications, from directory services to identity and access management platforms. User accounts serve a number of purposes, including user authentication, authorization, and accounting controls. An aggregated user account inventory can inform a wide array of administrative, operational, and technical security workflows. 	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Identity	Conditional Access	<p>A set of policies and configurations that control which users and devices have access to various services and data sources.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Multifactor Authentication	An authentication system which requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Privileged Access Management	Privileged access management (PAM) has to do with the processes and technologies necessary for securing privileged accounts. It is a subset of Identity and Access Management (IAM) that allows the control and monitor the activity of privileged users (who have access above and beyond standard users) once they are logged into the system.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Identity Federation & User Credentialing	Identity Federation is a way to login to one site using credentials from another. This way, the user only needs to remember one set of login information and does not have to worry about remembering multiple usernames and passwords. Instead, users can use a single credential to access all their online accounts. The most common identity providers are social media sites like Facebook and Google. There are also enterprise-level identity providers designed for use in business environments.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Behavioral, Contextual ID, and Biometrics	<p>Behavioral biometrics analyzes a user's digital physical and cognitive behavior to distinguish between cybercriminal activity and legitimate customers, identifying fraud and identity theft.</p> <p>Contextual ID consist in different identifiers for an "entity" (persons, objects, virtual values) based on the context without being able to completely identify the "entity" but still allowing the receiver to complete the authorization process as needed.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Identity	Least Privileged Access	The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Continuous Authentication	Continuous authentication constantly collects information about a user's actions and patterns of regular behavior and learns to distinguish between normal and abnormal behavior. Based on analysis of user behavior, access to a system can be granted	8(a) STARS III ALLIANT 2 VETS 2

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
		or additional user identity verification can be requested.	Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Identity	Integrated ICAM Platform	Identity, Credential, and Access Management (ICAM) is a set of security principles that helps organizations manage, monitor, and secure access to their resources. ICAM lets the right individuals access permitted resources for the right reasons, protecting organizations from unwanted access attempts.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Identity, Credentialing and Access Management SIN 541519ICAM Homeland Security Presidential Directive 12 and Service Components SIN 541519PIV Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Cloud SIN 518210C Software SIN 511210
Devices	Device Inventory	Device inventory refers to tracking and managing physical devices within an organization.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Devices	Device Detection and Compliance	<p>Device detection solutions identifies devices and their characteristics as they connect to networks, providing a continuous snapshot of active devices as well as the ability to act on device event information.</p> <p>Device compliance refers to the state of devices meeting the standards and regulations for the industry.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Devices	Device Authorization with Real Time Inspection	With input-constrained devices that connect to the internet, rather than authenticate the user directly, the device asks the user to go to a link on their computer or smartphone and authorize the device. This avoids a poor user experience for devices that do not have an easy way to enter text.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Devices	Remote Access	Remote access is the ability for an authorized person to access a computer or network from a geographical distance through a network connection.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Devices	Partially & Fully Automated Asset, Vulnerability, and Patch Management	<p>Patch management is the operational process of applying remediations (patches) to vulnerable systems.</p> <p>Vulnerability management is the process of identifying, scanning and prioritizing vulnerabilities for remediation.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Devices	Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	<p>Unified endpoint management is a class of software tools that provide a single management interface for mobile, PC and other devices. It is an evolution of, and replacement for, mobile device management and enterprise mobility management and client management tools.</p> <p>Mobile device management is the administration of mobile devices, such as smartphones, tablet computers, and laptops.</p>	ALLIANT 2 8(a) STARS III VETS 2 Enterprise Infrastructure Solutions (EIS) Wireless Mobility Solutions SIN 517312 Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Devices	Endpoint & Extended Detection & Response (EDR & XDR)	<p>Endpoint detection and response (EDR) solutions are designed to provide state of the art protection for endpoints.</p> <p>Extended Detection and Response (XDR) is designed to simplify enterprise network security management. XDR solutions integrate security visibility across an organization's entire infrastructure, including endpoints, cloud infrastructure, mobile devices, and more. This single pane of glass visibility and management simplifies security management and enforcement of consistent security policies across the enterprise.</p>	Software SIN 511210 ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Complex Commercial SATCOM Solutions (CS3) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Applications and Workloads	Application Inventory	<p>An application inventory is the complete list of applications or software assets owned by the company or institution. This includes all SaaS and On-Prem software.</p> <p>Application inventory can be developed into application landscape and visual diagrams. Usually created within Application Portfolio Management (APM) tools, it helps architects see how applications integrate with each other, which business capabilities they belong to, etc.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Applications and Workloads	Secure Software Development & Integration	Secure Software Development & Integration is the process of implementing, testing, and operating advanced software security techniques in compliance with technical reference architecture. Performing on-going security testing and code review to improve software security. Troubleshooting and debugging issues that arise.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Applications and Workloads	Software Risk Management	Software Risk Management is the utilization of fundamental risk management principles to identify, prioritize, remediate, and report security risks related to an organization's software infrastructure.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Highly Adaptive Cybersecurity Services SIN 54151HACS Cloud SIN 518210C

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Software SIN 511210
Applications and Workloads	Resource Authorization & Integration	<p>Resource-based authorization is a security technique used to limit access to resources and content in an application. It allows developers to create policies that determine who can access particular resources and how they are allowed to interact with them.</p> <p>Resource integration means matching a resource to a role in the target system and, if necessary, modifying the resource or providing supporting resources to allow it to play that role.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Homeland Security Presidential Directive 12 Product and Service Components SIN 541519PIV Cloud SIN 518210C Software SIN 511210
Applications and Workloads	Continuous Monitoring and Ongoing Authorizations	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. See organizational information security continuous monitoring and automated security monitoring.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Cloud SIN 518210C Software SIN 511210
Data	Data Catalog Risk Assessment	Data catalog risk assessment is a comprehensive data management framework to measure capabilities, and then identify and prioritize gaps, with a focus on auditability. Assessment scores help institutions align people, processes, technology, and data to better map and manage data risks.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Data	DoD Enterprise Data Governance	Discipline which is comprised of responsibilities, roles, functions, and practices supported by authorities, policies, and decisional processes which together administer data and information assets across a component to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			IT Professional Services SIN 54151S Software Maintenance Services SIN 54151
Data	Data Labeling and Tagging	<p>Data labeling refers to the process of adding tags or labels to raw data such as images, videos, text, and audio.</p> <p>These tags form a representation of what class of objects the data belongs to and helps a machine learning model learn to identify that particular class of objects when encountered in data without a tag.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Data	Data Monitoring and Sensing	Data monitoring, or real-time monitoring, is an oversight mechanism that monitors and ensures the quality of an organization's data. It includes data review processes to ensure data is complete, consistent, accurate, secure, and valid.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Cloud SIN 518210C Software SIN 511210
Data	Data Encryption & Rights Management	Data encryption is a method of protecting data confidentiality by converting it to encoded information, called ciphertext, that can only be decoded with a unique decryption key, generated either at the time of encryption or beforehand. Data encryption can be used during data storage or	8(a) STARS III ALLIANT 2 VETS 2

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
		<p>transmission and is typically used in conjunction with authentication services to ensure that keys are only provided to or used by authorized users.</p> <p>Rights management is the management of legal access to digital content. Various tools or technological protection measures like access control technologies, can restrict the use of proprietary hardware and copyrighted works.</p>	Enterprise Infrastructure Solutions (EIS) Cloud SIN 518210C Software SIN 511210
Data	Data Loss Prevention (DLP)	Data loss prevention is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Data	Data Access Control	Data access control is a fundamental security tool that enables the restriction of access based on a set of policies.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Cloud SIN 518210C Software SIN 511210

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Networks	Data Flow Mapping	<p>Data Flow is the journey of data from the point of collection to where it flows to third parties throughout the organization.</p> <p>Understanding the data flow allows us to map the data journey and enable businesses to manage and secure their customers' data fairly and securely. Implementing any type of security is difficult without thoroughly understanding the data lifecycle.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210
Networks	Software Defined Networking (SDN)	Software-defined networking (SDN) technology is an approach to network management that enables dynamic, programmatically efficient network configuration in order to improve network performance and monitoring, in a manner more akin to cloud computing than to traditional network management.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210
Networks	Macro-segmentation	Macro-segmentation breaks up a network into groups of systems, providing the ability to divide network infrastructure and systems based upon departments or other criteria. It is typically implemented using VLANs and firewalls.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210
Networks	Micro-segmentation	Micro-segmentation usually divides an organization's infrastructure at the system or even the application level. It is used to provide highly granular visibility and control over data flows within an organization's network, enabling the implementation of a zero trust security strategy. It is often deployed using software-defined solutions because these systems already require deep visibility and control for routing purposes (making inspection and policy enforcement easier)	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Policy Decision Point (PDP) & Policy Orchestration	Mechanism that examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration.	ALLIANT 2 8(a) STARS III VETS 2

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
		A policy orchestration platform typically provides a range of features that support the creation and management of security policies. This can include risk analysis, compliance reporting, and event correlation and analysis, as well as automated enforcement and remediation.	Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Critical Process Automation	Process automation refers to the use of technology to automate repetitive and manual tasks within a business process. It includes technologies like robotic process automation (RPA) or intelligent document processing (IDP), workflow orchestration, artificial intelligence (AI), system integrations, and business rules. The goal of process automation is to reduce the need for human intervention in time-consuming, routine tasks for more efficient and effective processes.	ALLIANT 2 8(a) STARS III VETS 2 Enterprise Infrastructure Solutions (EIS) Automated Contact Center Solutions SIN 561422 Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Machine Learning	Machine learning is a branch of artificial intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy.	ALLIANT 2 8(a) STARS III VETS 2 Enterprise Infrastructure Solutions (EIS) Automated Contact Center Solutions SIN

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			561422 Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Artificial Intelligence	Artificial intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems.	ALLIANT 2 8(a) STARS III VETS 2 Enterprise Infrastructure Solutions (EIS) Automated Contact Center Solutions SIN 561422 Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Security Orchestration, Automation & Response (SOAR)	Security Orchestration, Automation & Response (SOAR) is a software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Software SIN 511210
Automation and Orchestration	API Standardization	<p>API Standardization helps ensure that API definitions comply with a company's API style guide. API design is the creation of an effective interface that allows you to better maintain and implement the API, while enabling consumers to easily use this API.</p> <p>Consistent API design is standardizing the design, across all APIs, and the resources they expose, within an organization or team. It is a common blueprint for developers, architects, and technical writers to follow, to ensure a consistent "voice", brand, and experience in the API consumption. Organizations standardize design using Style Guidelines that aim to ensure consistency in the way APIs are designed and implemented.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) IT Professional Services SIN 54151S Cloud SIN 518210C Software SIN 511210
Automation and Orchestration	Security Operations Center (SOC) & Incident Response (IR)	<p>Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.</p> <p>Incident response is an organized, strategic approach to detecting and managing cyber-attacks in ways that minimize damage, recovery time and total costs.</p>	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Visibility and Analytics	Log All Traffic (Network, Data, Apps, Users)	Traffic logs are produced whenever traffic hits a rule which has been enabled for logging. Incoming or outgoing traffic through a device is filtered by rules that either allow or disallow (deny) the traffic. For every event that is allowed or denied by a rule enabled for logging, a traffic log is written on the designated log server.	Software SIN 511210 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Highly Adaptive Cybersecurity Services SIN 54151HACS Identity, Credentialing and Access Management SIN Identity, Credentialing and Access Management SIN 541519ICAM Cloud SIN 518210C Software SIN 511210
Visibility and Analytics	Security Information and Event Management (SIEM)	Security information and event management (SIEM) is a field within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Highly Adaptive Cybersecurity Services SIN 54151HACS Identity, Credentialing and Access Management SIN Identity, Credentialing and Access Management SIN 541519ICAM Cloud SIN 518210C

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
Visibility and Analytics	Common Security and Risk Analytics	Security and risk analysis is one step in the overall cybersecurity risk management and risk assessment process. The analysis entails examining each risk to the security of your organization's information systems, devices, and data and prioritizing the potential threats.	Software SIN 511210 8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Visibility and Analytics	User and Entity Behavior Analytics	User and entity behavior analytics (UEBA) is a cybersecurity solution that uses algorithms and machine learning to detect anomalies in the behavior of not only the users in an enterprise network but also the routers, servers, and endpoints in that network.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Cloud SIN 518210C Software SIN 511210
Visibility and Analytics	Threat Intelligence Integration	A threat intelligence platform automates the collection, aggregation, and reconciliation of external threat data, providing security teams with the most recent threat insights to reduce threat risks relevant for their organization.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Wireless Mobility Solutions SIN 517312 Cloud SIN 518210C Software SIN 511210
Visibility and Analytics	Automated Dynamic Policies	Automated dynamic policy enables the system to adjust the policies according to the changing circumstance, and makes the system more flexible and adaptive.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM Purchasing of New Electronic Equipment SIN 33411

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications Solutions SIN 517410 Cloud SIN 518210C Software SIN 511210
Governance	Documentation Development	Document Development Life Cycle is a systematic process that enables document creation in a specific order to create easy-to-understand content for the users and simplify complex topics. Documentation development in system engineering is the umbrella term that encompasses all written documents and materials dealing with System Development Life Cycle (SDLC).	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Public Key Infrastructure Shared Service Providers Program SIN 541519PKI Automated Contact Center Solutions SIN 561422
Governance	Policy Enforcement	Policy enforcement in data security refers to the process of ensuring that the security policies and procedures implemented by an organization are followed consistently by its employees, partners, and stakeholders.	8(a) STARS III ALLIANT 2 VETS 2

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
			Enterprise Infrastructure Solutions (EIS) Electronic Commerce and Subscription Services SIN 54151ECOM Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151 Commercial Satellite Communications Solutions SIN 517410
Governance	Compliance Monitoring	Compliance monitoring is the process that ensures organizations meet the policies and procedures to identify compliance risk issues in their day-to-day operations and functions.	8(a) STARS III ALLIANT 2 VETS 2 Enterprise Infrastructure Solutions (EIS) Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151
Governance	Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other	8(a) STARS III ALLIANT 2

Pillar Cross-Cutting Capability	Component	Component Description	GSA Technology Purchasing Program
		organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.	VETS 2 Enterprise Infrastructure Solutions (EIS) 2GIT PRODUCTS Purchasing of New Electronic Equipment SIN 33411 Highly Adaptive Cybersecurity Services SIN 54151HACS IT Professional Services SIN 54151S Software Maintenance Services SIN 54151

Appendix B – References

This buyer’s guide is developed in accordance with the following references:

References
Executive Order (EO) 14028, Improving the Nation’s Cybersecurity, May 12, 2021
Office of Management and Budget (OMB) M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022
Department of Defense (DoD) Zero Trust Strategy, October 21, 2022
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 Zero Trust Architecture, August 2020
Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0, April 2023

Appendix C – GSA Vehicle Reference

Multiple Award Schedule – Information Technology

Multiple Award Schedule (MAS) Information Technology (IT) shortens procurement cycles, ensures compliance, and delivers the best value on over 7.5 million innovative IT products, services, and solutions from over 4,600 pre-vetted vendors. It offers federal, state, local and tribal governments innovative solutions for their information technology needs. Below are the MAS IT Solutions and Special Item Numbers (SINs) categorized based on government mandates, industry evolution, and buying trends that have been identified:

- **Electronic Commerce**

- Electronic Commerce (SIN 54151ECOM)

- **IT Hardware**

- Leasing of new electronic equipment (SIN 532420L)

- Purchasing of New Electronic Equipment (SIN 33411)

- Maintenance of Equipment, Repair Services and/or Repair/Spare Parts (SIN 811212)

- **IT Services**

- Health IT Services (SIN 54151HEAL)

- Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS)

- IT Professional Services (SIN 54151S)

- **IT Software**

- Software Licenses (SIN 511210)

- Software Maintenance Services (SIN 54151)

- **IT Solutions**

- Automated Contact Center Solutions (SIN 561422)

- Cloud and Cloud-Related IT Professional Services (SIN 518210C)

- Earth Observation Solutions (EOS) (SIN 541370GEO)

- Identity, Credential and Access Management (ICAM) (SIN 541519ICAM)

- Public Key Infrastructure (PKI) Shared Services Provider (SSP) Program (SIN 541519PKI)

- Homeland Security Presidential Directive 12 Product and Service Components (SIN 541519PIV)

- **IT Training**
Training Courses (SIN 611420)
- **IT Telecommunications**
Wireless Mobility Solutions (SIN 517312)
Commercial Satellite Communications COMSATCOM Transponded Capacity (SIN 517410)

Source: <https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology>

Defense Enterprise Office Solutions (DEOS)

Defense Enterprise Office Solutions (DEOS) represents an enterprise-based set of capabilities that include: productivity tools such as word processing and spreadsheets, email, collaboration, file sharing, and storage. Its intended environments are Microsoft 365 instantiation in a DoD Impact Level 5 (Unclassified) and Impact Level 6 (Classified) cloud operating within the United States and overseas providing capability to support garrison and network challenged operations.

2nd Generation IT Blanket Purchase Agreements

2nd Generation IT (2GIT) includes pre-competed commercial hardware, software, and ancillary services such as:

- Purchase of New Equipment
- Maintenance of Equipment, Repair Services and/or Repair/Spare Parts
- Software License - Term Software & Perpetual
- Software Maintenance Services
- Order-Level Materials (OLM)

2nd Generation IT Products hardware and software BPAs offer:

- Access to mission-critical, best-value IT from a diverse pool of more than 70 industry partners including more than 50 small businesses.
- Solutions that meet current procurement policies, incorporate best practices (like collecting prices paid data), and track savings.
- Options that support the FY19 SECURE Technology Act and other federal cybersecurity efforts.

Source: <https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/multiple-award-schedule-it/2git-bpa>

Governmentwide Strategic Solutions Blanket Purchase Agreements

Governmentwide Strategic Solutions for Desktops and Laptops are blanket purchase agreements with standard configurations for desktop and laptop computers, including:

- Access to solutions from pre-vetted vendors in every small business socio-economic category.
- Acquisition and technology guidance from our subject matter experts.
- Competitive, flexible pricing structures and opportunities to negotiate for further discounts.
- Customized terms and conditions at task order level and master contract level.
- Reduced lead times and simplified service procurement processes that put you in control.
- Standard configuration specifications that are refreshed every nine months based on industry updates and customer feedback

Source: <https://www.gsa.gov/technology/technology-purchasing-programs/mas-information-technology/buy-from-mas-information-technology/order-desktops-and-laptops-through-mas>

Governmentwide Acquisition Contracts (GWAC)

GWACs are cost-effective, innovative solutions for IT requirements available to the federal government. GWACs provide access to pre-competed Best-in-Class IT solutions including: System Design; Software Engineering; Information Assurance; and Enterprise architecture solutions. Below are the GWACS contracts:

- 8(a) STARS III
- Alliant 2
- VETS 2 (SDVOSB)

Source: <https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/gwacs>

Telecommunications and Network Services

Telecommunications and Network Services provides cost-effective communications infrastructure and network needs. Below are the telecommunication and network services contracts:

- Enterprise Infrastructure Solutions (EIS)
- Satellite Communications (SATCOM)
- Enterprise Mobility
- Relay

Source: <https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services>

Appendix D –Zero Trust Reference Architecture

The below diagram depicts an industry standard logical ZTA. **Note:** Not all of the components listed in Appendix A are listed in this Zero Trust Reference Architecture. Only core components are listed due to space limitations.

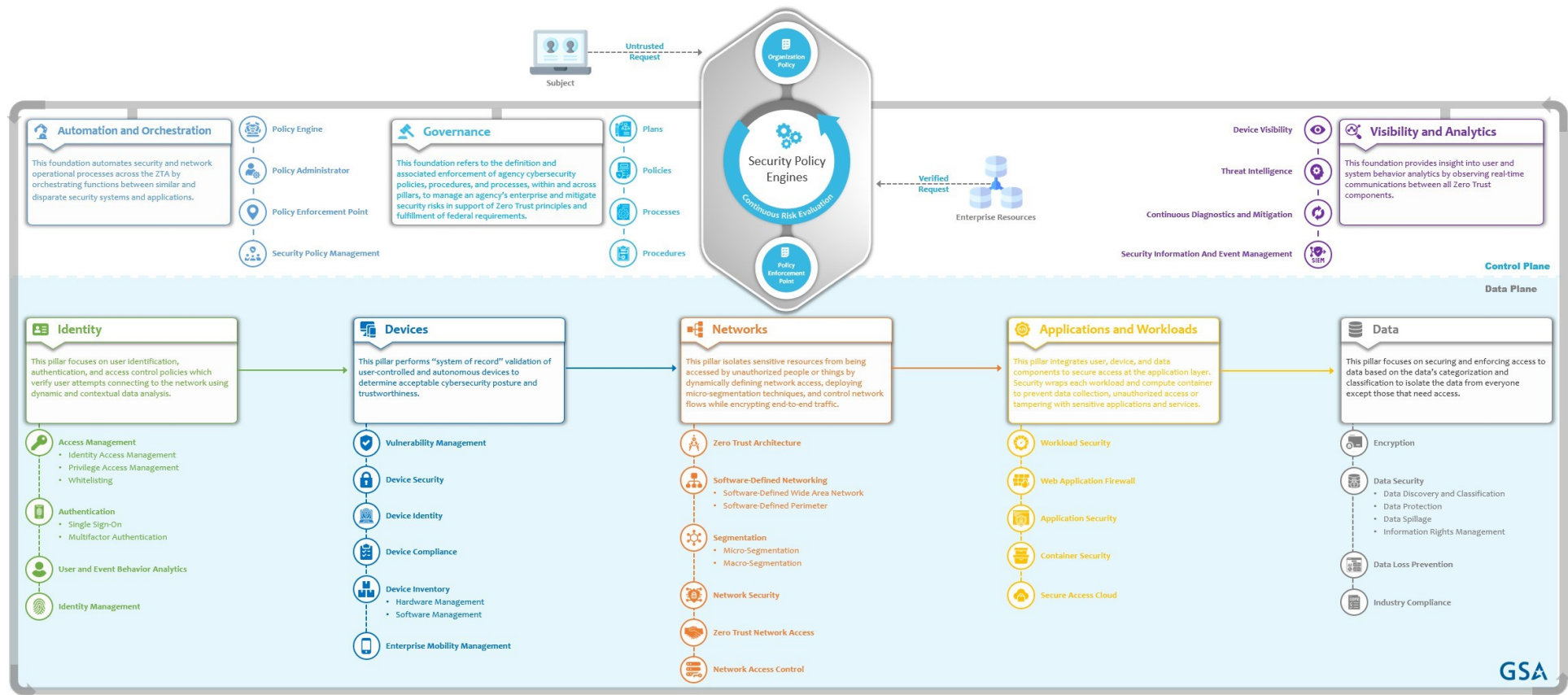


Figure 2- Zero Trust Reference Architecture