Introduction

The General Services Administration (GSA) is issuing this Request for Information (RFI) to conduct market research in the vendor community seeking vendor capabilities in the areas of Zero Trust Architectures and Zero Trust Networking (Zero Trust).

This RFI is issued for information and planning purposes only and does not constitute a solicitation nor does it restrict the government to any future acquisition approach. In accordance with Federal Acquisition Regulation (FAR 15.201(e)), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. The purpose of this RFI is to obtain market information on sources of supply, industry practices, and recommendations for design solutions for Federal Government entities desiring to implement components of Zero Trust. The Government is not responsible for any cost incurred by industry in furnishing this information. All costs associated with responding to this RFI will be solely at the interested vendor's expense. Not responding to this RFI does not preclude participation in any future Request for Proposal (RFP), if any is issued. Any information submitted by respondents to this RFI is strictly voluntary.

Information gained from this RFI will be used to develop informational products to inform cross-government security professionals. No RFP is expected to result from this request.

Zero Trust concepts have been around for several years now, however, Federal demand for information and the potential to implement the principles of Zero Trust is currently high. Additionally, GSA anticipates that there are many vendors who have products and solutions that are available to assist the Federal Government with implementing the principles of Zero Trust, so this RFI is an effort to gather that information. GSA will coordinate all information received and correlate it into a matrix which will be made available across Government and will be used as a reference for Government entities looking to implement the principles of Zero Trust. GSA will essentially marry the information received from the vendor community with Federal guidance (NIST 800-53, NIST Draft 800-207, DHS Continuous Diagnostics and Mitigation (CDM) etc.), and make it available to any interested Federal Government entity. The goals of supplying this information to Federal Government entities include:

1) Educating the Federal Government on the vendor products and solutions available to them to assist in implementing Zero Trust designs,

2) Organizing and correlating the information received into a reference matrix to be used by Federal Government entities to assist them with selecting products and solutions targeted at specific focus areas within their network, and

3) Improving the overall posture of cybersecurity within the Federal Government with more modernization based on the principles of Zero Trust.

Background

In May 2018, the Federal CIO Council Services, Strategy, and Infrastructure Committee asked ACT-IAC to evaluate the technical maturity, availability for procurement, and other important issues related to the potential federal agency adoption of Zero Trust. The project's approach included two phases. Phase 1 was to provide some initial market research, presentations and demonstrations, and evaluation of the underlying trust algorithms of Zero Trust. That phase has been completed and results of the research were summarized in a report "Zero Trust Cybersecurity Current Trends" released April 18, 2019. Phase 2 is now underway, and this phase aims at evaluating the maturity of Zero Trust capabilities against industry products and solutions. GSA is conducting research for Phase 2 of this project and is conducting a market survey requesting vendors to provide responses on how their products and solutions align with specific Zero Trust policies/requirements AND share current and future use cases as examples of implementation.

This market research will be conducted by asking seven questions, and respondents are free to respond to as many of them as they'd like. For guidance, GSA recommends that vendor respondents answer, at a minimum:

- Either Question 1 OR Question 2, AND
- Either Question 3 OR Question 4, AND
- Either Question 5 OR Question 6, AND
- Question 7.

Following the collection of the vendor information, an analysis and correlation will be performed to:

1. Map vendor’s Zero Trust products and solutions against the ACT-IAC Zero Trust pillars,
2. Map vendor’s Zero Trust products and solutions against the NIST draft 800-207 publication,
3. Map vendor’s Zero Trust products and solutions to DHS CDM guidelines, and
4. Map vendor’s Zero Trust products and solutions against NIST SP 800-53 controls.

Market Research: Documenting capabilities and alignment with Zero Trust Principles

Question 1: How do your company’s products/solutions align with the “pillars” of Zero Trust as described in the ACT-IAC Zero Trust white paper dated April 18, 2019?

(https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf)

Consider responding in the simplified table format shown below:

ACT-IAC Zero Trust Pillar	Vendor Product or Solution	Description of how your product meets the capabilities of the Pillar

For convenience, below is an excerpt from the ACT-IAC Zero Trust white paper specific to identifying the pillars of Zero Trust and the definitions and capabilities within each:

Fundamental Pillars of Zero Trust

Zero Trust can be thought of as a strategic initiative that, together with an organizing framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations. ZT efforts need to incorporate, coordinate, and integrate a challenging combination of policies, practices, and technologies to succeed. A conceptual security model can be helpful to understand and organize those components (see Figure 1 for an example of a zero trust security model).

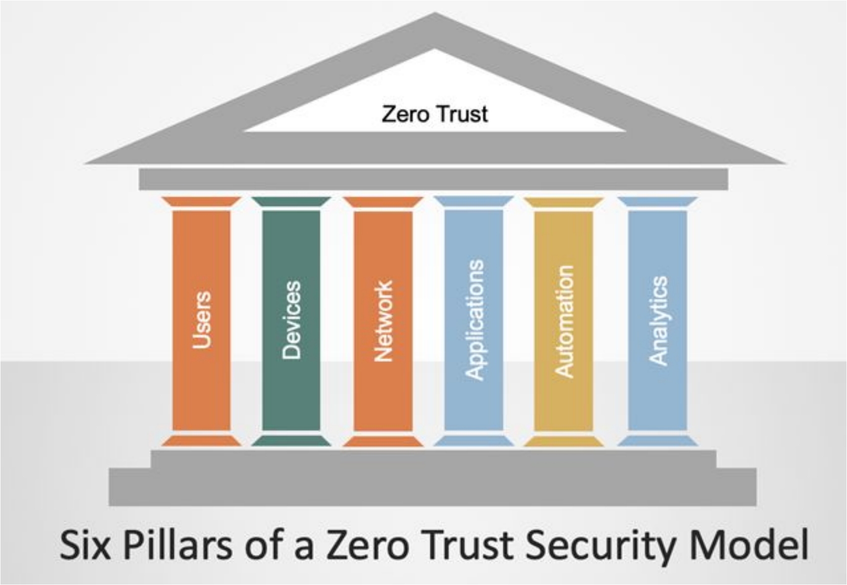

Figure 1 *- Six Pillars of a Zero Trust Security Model*

Pillar #1 – User - People/Identity Security

Ongoing authentication of trusted users is paramount to ZT. This encompasses the use of technologies like Identity, Credential, and Access Management (ICAM) and multi-factor authentication and continuously monitoring and validating user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions, such as traditional web gateway solutions, are also important.

Pillar #2 – Devices - Device Security

Real-time cybersecurity posture and trustworthiness of devices is a foundational attribute of a ZT approach. Some "system of record" solutions such as Mobile Device Managers provide data that can be useful for device-trust assessments. In addition, other assessments should be conducted for every access request (e.g. examinations *of compromise state, software versions, protection status, encryption enablement, etc.).*

Pillar #3 – Network - Network Security

Some argue that perimeter protections are becoming less important for networks, workflows, tools and operations. This is not due to a single technology or use-case, but rather a culmination of many new technologies and services that allow users to work and communicate in new ways. Zero Trust Networks are sometimes described as "perimeterless", however this is a bit of a misnomer. Zero Trust Networks actually attempt to move perimeters in from the network edge and segment and isolate critical data from other data. The perimeter is still a reality, albeit in much more granular ways. The traditional infrastructure firewall perimeter "castle and moat" approach is not sufficient. The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls. Network security is expanding as agencies grow their networks to partially or fully transition to Software Defined Networks, Software Defined Wide Area Networks and internet-based technologies. It is critical to (a) control privileged network access, (b) manage internal and external data flows, (c) prevent lateral movement in the network, and (d) have visibility to make dynamic policy and trust decisions on network and data traffic. The ability to segment, isolate, and control the network continues to be a pivotal point of security and essential for a Zero Trust Network.

Pillar #4 – Applications - Application and Workload Security

Securing and properly managing the application layer as well as compute containers and virtual machines is central to ZT adoption. Having the ability to identify and control the technology stack facilitates more granular and accurate access decisions. Unsurprisingly, multi-factor authentication is an increasingly critical part of providing proper access control to applications in ZT environments.

Pillar #5 – Automation - Security Automation and Orchestration

Harmonious, cost effective ZT makes full use of security automation response tools that automate tasks across products through workflows while allowing for end-user oversight and interaction. Security Operation Centers commonly make use of other automated tools for security information and event management and user and entity behavior analysis. Security orchestration connects these security tools and assists in managing disparate security systems. Working in an integrated manner, these tools can greatly reduce manual effort and event reaction times and reduce costs.

Pillar #6 – Analytics - Security Visibility and Analytics

You cannot combat a threat you cannot see or understand. ZT leverages tools like security information management, advanced security analytics platforms, security user behavior analytics, and other analytics systems to enable security experts to observe in real time what is happening and orient defenses more intelligently. The focus on the analysis of cyber-related event data can help develop proactive security measures before an actual incident occurs.

Question 2: How are the Zero Trust Tenants (cited inside of “Draft” NIST Special Publication 800-207 “Zero Trust Architecture”) realized through the use of your products?

Leveraging the latest draft of NIST SP 800-207, Zero Trust Architecture, describe your company’s approach to the Zero Trust tenants defined below:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location. Network location does not imply trust. Access to individual enterprise resources is granted on a per-session basis.
3. Trust in the requester is evaluated before the access is granted.
4. Access to resources is determined by dynamic policy — including the observable state of client identity, application, and the requesting asset — and may include other behavioral attributes.
5. The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible. No device is inherently trusted.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communication.
7. The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture

Question 3: Where do your products fit into the logical design of a Zero Trust Architecture as documented in the latest draft of NIST SP 800-207 “Zero Trust Architecture”?

Describe in detail where each of your products fit into the logical Zero Trust Architecture as described in the latest draft of NIST 800-207, Zero Trust Architecture. For each component, itemize which of your products/solutions apply.

Implements/Enforces: Your product implements a feature which is central to delivering the capability provided for this architectural component in the majority or in whole.

Supports/Enhances: Your product implements a feature which is central to delivering the capability provided for this architectural component but does not provide the majority of the capability required for this component.

Integrates with 3rd Party: Your product or solution requires the support of a 3rd party product or solution to implement this component.

Plays no Role: Your product or solution does not enforce or support this capability, nor does your product or solution require information from nor integrate with solutions within this component.

Architecture Component	Product Action		Vendor Response
Policy Engine	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		

Policy Administrator	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Subject	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
System	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Policy Enforcement Point	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Enterprise Resource	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		

	Plays no Role		
CDM System	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Industry Compliance	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Threat Intelligence	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Activity Logs	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
Data Access Policy	Implements/Enforces		
	Supports/Enhances		

	Integrates with 3rd Party		
	Plays no Role		
PKI	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
ID Management	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		
SIEM System	Implements/Enforces		
	Supports/Enhances		
	Integrates with 3rd Party		
	Plays no Role		

Question 4: How do your products implement and operationalize Zero Trust (refer to sections 3.1 and 3.2 of draft NIST SP 800-207 “Zero Trust Architecture”?

Section 3.1 and Section 3.2 of the latest draft of NIST 800-207, Zero Trust Architecture, outlines variations of how Zero Trust solutions create policies and how those policies are enforced within workflows. The table below represents a matrix of the NIST policy creation mechanisms and enforcement variations. Please use your understanding of Zero Trust and place all your applicable products and services within this matrix. Please identify your product or solution, include the source or sources for the relevant policy creation mechanism, and describe how this data is deployed to enforce Zero Trust principles.

Don’t feel constrained by the table. Feel free to reference the matrix location (e.g. GOV-C) in your response header. Use as many specific matrix locations as necessary to cover your suite of products. If you don’t believe NIST adequately captures a policy creation or deployment mechanism feel free to describe your own. Please include specifics on where your solution is different than the NIST descriptions

Policy Creation Mechanism	**Deployment/Enforcement Mechanism**				
	Device Agent/Gateway-Based	Enclave-Based	Resource Portal-Based	Device Application Sandboxing	{OTHER}
Identity Governance	GOV-A	GOV-B	GOV-C	GOV-D	GOV-O
Micro-Segmentation	SEG-A	SEG-B	SEG-C	SEG-D	SEG-O
Network Infrastructure and Software Defined Perimeters	PER-A	PER-B	PER-C	PER-D	PER-O

{Other Mechanism}	OTH-A	OTH-B	OTH-C	OTH-D	OTH-O

Question 5: How do your products/solutions align with the Zero Trust Pillars when mapped with the DHS Continuous Diagnostics and Mitigation (CDM) capabilities?

The Zero Trust pillars introduce a framework that is reflected in the Continuous Diagnostics and Mitigation (CDM) program. The Department of Homeland Security developed the CDM program to support government-wide and agency-specific efforts to implement adequate and risk-based cybersecurity. The program completion is based on four phases Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.

The table below maps the Zero Trust Pillars to the DHS CDM capabilities from these four phases. While the capabilities align with the Zero Trust framework, the boundaries of each definition are fluid. Please use the table below to align your products and solutions to one or more CDM capability. An additional pillar for “data” has been added to the table below.

Zero Trust Pillars	CDM Capabilities	Description	Vendor Product
Users	**Manage Trust in People Granted Access**	Assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.	

	Manage Security-Related Behavior	Ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.	
Devices	**Hardware management**	Discover unauthorized or unmanaged hardware on a network.	
	Software Management	Discover unauthorized or unmanaged software on a network.	
	Configuration Settings Management	Ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.	
	Vulnerability Management	Discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.	
Network	**Credentials and Authentication Management**	Ensures that only proper credentials are authenticated to systems, services, and facilities.	
	Managing Privileged User Access Capability	Provides an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	
	Network Protection	Limits, prevents, and/or allows the removal of unauthorized network connections/access via devices such as firewalls that sit at a boundary and regulate the flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries and	

		addresses physical access systems that limit unauthorized user physical access to Federal Government facilities.	
Applications	**Credentials and Authentication Management**	Ensures that only proper credentials are authenticated to systems, services, and facilities.	
	Managing Account Access Capability	Provide an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	
	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.	
Automation	**Manage Events**	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.	
	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).	
Analytics	**Data Protection**	Provides data protection functions through cryptography, masking/obfuscation, or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to	

		data, functions, and privilege abuse) and provide context for security investigations.	
Data	**Data Discovery and Classification**	Supports data protection functions through data identification, data classification, and data tagging.	
	Data Loss Prevention	Provides data protection functions through data loss prevention capabilities, to include data protection policy management and data protection security orchestration.	
	Data Protection	Provides data protection functions through cryptography, masking/obfuscation, or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.	
	Data Spillage	Provides data breach/spillage response actions.	
	Information Rights Management	Provides data protection functions through information rights management capabilities using fine-grained access control to encrypted data.	

Question 6: Identify how your zero trust products and solutions can be utilized to implement NIST 800-53 security controls.

The Risk Management Framework (800-37) and the draft of NIST 800-53 r 5 (draft) specifies that control tailoring is appropriate for different communities of interest. In order to meet the goals and objectives of achieving a Zero Trust architecture, provide additional information as to the main controls that your products and solutions support.

Vendors should consider responding with how the control is met. Options are:

- **Implements/Enforces:** Your product or solution implements a feature which enforces this control in whole.
- **Supports/Enhances:** Your product implements a feature which is central to enhancing or enforcing this control, but typically does this alongside other vendor products solutions.
- **Integrates with 3rd Party:** Your product or solution typically utilizes the support of a 3rd party product or solution to implement this control enforcement.
- **Plays no Role:** Your product or solution does not enforce or support this control, nor does your product or solution provide information to a 3rd-party to enforce this control.

Below is a table identifying a sampling of the security controls listed in NIST 800-53 with some sample text to be used as an example. The complete table of controls is available in the NIST 800-53 publication.

Class	Family	Number	Title	Y/N	Product/Explanation
Technical	Access Control	AC-1	Access Control Policy and Procedures	N	Product XYZ plays no role in this control.

Technical	Access Control	AC-2	Account Management	Y	Product XYZ implements this control by…
Operational	Configuration Management	CM-2	Baseline Configuration	Y	Product XYZ supports and enhances this control by…
Technical	Identification and Authentication	IA-3	Device Identification and Authentication	Y	Product XYZ integrates with other products to support this control by…

Market Research: Demonstrating Product and Solution Effectiveness through Use Cases

Question 7: Provide descriptions and references for no more than three currently implemented use cases (preferably of environments of 10,000+ end users) that leverage your products and services in a Zero Trust architecture. If any of your use cases requires integration with other 3rd party products to demonstrate its Zero Trust capabilities, please provide details.

GSA is interested in better understanding the Zero Trust use cases for your products and solutions. Vendors should review section 3.4.1 Network Requirements to Support ZTA of NIST 800-207 (DRAFT), and ensure that your use case descriptions provide specific evidence of how these requirements are met with clear identification of any 3rd-party products where your solution does not support the requirement as a stand-alone product. Please include in your response:

- A title for your use case (some examples from NIST 800-207 include ”Enterprises with Satellite (Remote) Facilities”, “Multi-cloud Enterprises”, and “Enterprises with Contracted Services and/or Nonemployee Access”,
- Customer name and/or industry
- Reference POC
- Budget
- Implementation timeline and details
- Problem statement
- Solution description (include size: number of end users, endpoints, resources, etc)
- Technologies utilized
- Details of integration with 3rd party products
- Evidence of network requirements met
- Lessons learned

Please use the list of questions below to assist in shaping your response to Requirement/Question 7 .

- Was any testing of your product/solution done prior to implementation? If yes, how was this accomplished?
- Was any technology “retired” during the process of implementing your products/solutions?
- Was the technology that you deployed a “net new” product to your client’s infrastructure OR was it a re-purpose of some existing technology OR was it a replacement to other products that were already in the network?
- Which industry sector do you see more / an increasing number of ZT strategy implementations?

RFI Response Questions and Instructions

Please provide your company’s response to the seven questions listed in the RFI by close of business on Tuesday, June 30, 2020.   The questions are summarized below:

Architectural Concepts (please respond to at least one)

Question 1: How do your company’s products/solutions align with the “pillars” of Zero Trust as described in the ACT-IAC Zero Trust white paper dated April 18, 2019?

Question 2: How are the Zero Trust Tenants (cited inside of “Draft” NIST Special Publication 800-207 “Zero Trust Architecture”) realized through the use of your products?

Operational Concepts (please respond to at least one)

Question 3: Where do your products fit into the logical design of a Zero Trust Architecture as documented in the latest draft of NIST SP 800-207 “Zero Trust Architecture”?

Question 4: How do your products implement and operationalize Zero Trust (refer to sections 3.1 and 3.2 of draft NIST SP 800-207 “Zero Trust Architecture”?

Mapping to Other Frameworks (please respond to at least one)

Question 5: How do your products/solutions align with the Zero Trust Pillars when mapped with the DHS Continuous Diagnostics and Mitigation (CDM) capabilities?

Question 6: Identify how your zero trust products and solutions can be utilized to implement NIST 800-53 security controls.

Use Cases (please respond to this one)

Question 7: Provide descriptions and references for no more than three currently implemented use cases (preferably of environments of 10,000+ end users) that leverage your products and services in a Zero Trust architecture. If any of your use cases requires integration with other 3rd party products to demonstrate their Zero Trust capabilities, please provide details.

Questions from vendors will be received up to one week from RFI posting. GSA reserves the right to not respond to any, all, or select responses of materials submitted. Please submit any inquiries, or questions concerning this announcement, to cyberportfolio@gsa.gov via email. Interested parties shall also provide the following information in their responses:

- Company Name
- Company Address
- Point of contact name
- Telephone number
- Email address

Please be direct and concise in your responses. Responses are due by close of business on Tuesday June 30, 2020. GSA appreciates the time and anticipated responses from all interested vendors.

How to Submit a Response

- Email response to: cyberportfolio@gsa.gov
- Title response: “Zero Trust RFI - [Vendor Name]”
- Format: Return responses in Microsoft Word format
- Include in addition to requested questions responses:
  - Company Name
  - Company Address
  - Point of Contact Name
  - Point of Contact Telephone Number
  - Email Address

Note: GSA may reach out (via phone/email) after the RFI closes to dive deeper into responses to better understand the information submitted. GSA reserves the right to connect with some respondents, all respondents, or none.

Information gained from the RFI will be used by GSA and also shared with ACT-IAC for the creation of no-cost informational products designed to help federal CISOs make informed decisions.