REQUEST FOR INFORMATION (RFI)

With increasing numbers of users located outside the protections of network security appliances at the Defense Information Systems Network (DISN) boundary, there exists a new requirement to ensure the security of both the DISN and the customers who utilize Defense Information Systems Agency (DISA) services. Many current network security technologies were not designed to handle modern day security threats, which has forced DISA to utilize multiple products to handle a variety of security requirements. These products apply a "defense in depth" approach but are siloed and not optimized to provide a high performance end to end secure connection. The network has not been architected to quickly apply zero trust security principles and adapt to the changes in how users need to access their applications and data.

Software Defined Wide Area Network (SD WAN) technology is an emerging concept that can have massive effects on how we rapidly deploy networks, prioritize traffic, and continuously monitor performance. This can be paired with a number of different security technologies that can give the DoD a true zero trust network.

Secure Access Service Edge (SASE) is the convergence of wide area networking and network security services, into a single, cloud-delivered service model. It applies secure access based on the user, the user's identity, location or device. It leverages commercially-available solutions. Containerized application security stacks augment SASE solutions to achieve enhanced conditional access and implement data centric security protections. These work in conjunction with enterprise security enablers, such as Public Key Infrastructure (PKI)/Identity Control Access Management (ICAM), endpoint, Big Data Platform (BDP), and DevSecOps into a single, consolidated service model. It leverages commercially available solutions to apply secure access control decisions based on the user, location, and device status for complete end to end security in alignment with zero trust principals.

DISA plays a critical role in providing network and security services across the Department of Defense (DOD), and will architect and deploy zero trust concepts to enable secure, conditional and continuous access. These capabilities will enable DISA to continue to provide secure networking solutions to their customers who access to DOD resources from a variety of locations and platforms to better support the Department's mission.

THIS IS A REQUEST FOR INFORMATION (RFI) NOTICE ONLY. THIS IS NOT A REQUEST FOR PROJECT PROPOSAL (RFPP). NO SOLICITATION IS AVAILABLE AT THIS TIME. NO AWARD WILL BE MADE AS A RESULT OF THIS RFI. THE GOVERNMENT WILL NOT PAY FOR ANYTHING CREATED AS A RESULT OF THIS RFI.

1. OVERVIEW/PURPOSE/DESCRIPTION OF PROCUREMENT:

DISA is planning the procurement of tools/systems/capabilities, which will assist in deploying a zero trust SASE capability, integrated software defined (SD) Wide Area Network (WAN) technology, Customer Edge Security Stacks, and Application Security Stacks on both the SIPRNet and NIPRNet. **DISA seeks industry feedback on the projected acquisition approach**.

The Government desires a new approach to deliver an initial, minimum viable product (MVP) for the architecture of a SASE cloud-based, Zero Trust network solution within six months of award and delivering a second MVP for the inclusion of the SD-WAN with Customer Edge Security Stack prototypes within twelve months of award. Improvement and operational implementation of these capabilities through the year 2025 are planned. DISA expects the performing vendor(s) to play a critical role interacting with key stakeholders across DISA and the Fourth Estate. It is anticipated that there will

be 1-2 partner organizations for inclusion in the scope of the MVP.

The Government is planning to develop these capabilities by implementing key Zero Trust concepts within the SASE security framework. These are new operational capabilities for the DOD that will significantly improve routing and security services. The Government intends to prototype several tools and processes through the execution of this project leveraging commercial best practices where applicable. Specifically, the Government intends to apply this development activity to create, design, develop, demonstrate the operational utility of SASE, Customer Edge Security Stacks at the DISN Customer Edge Point of Presence (PoP), scalable Application Security Stacks deployed in front of one or more application workloads, and SD-WAN integration, including the ability to provide micro segmentation and the prioritization of specific of traffic flows. These capabilities will integrate with existing DISA systems (e.g. ICAM, Comply to Connect, Endpoint systems, SIEM, BDP, etc.) to provide conditional access and policies to limit functionality based on user and endpoint attributes, and policies based on application and data tagging. From a process perspective, the Government intends to pilot, and subsequently operationalize these secure networking and security functions on both NIPRNet and SIPRNet.

The Government is considering the use of an Other Transaction Authority (OTA) for the Prototype, in order to support this unique acquisition. Additionally, the Government is considering instituting a Challenge Based Acquisition (ChBA) to understand industry capabilities and to reduce execution risk early in the process. To implement ChBA, the Government would provide short challenge scenarios prior to awarding an OTA, enabling industry partners to demonstrate their technical capabilities, as they specifically apply to this procurement. For more information on ChBA, please reference the ChBA guide at: https://www.mitre.org/publications/technical-papers/challenge-based-acquisition-5th-edition.

Additionally, the Government is exploring options for a Reverse Industry Day as a result of this RFI. If the Government pursues a Reverse Industry Day, the Government may limit the number of participants. Those companies selected to participate in the reverse industry day will be given the opportunity to provide a presentation on their capabilities referenced in their RFI responses.

Through responses provided to this RFI, the Government intends to obtain the following information:

- Industry's capability to meet the acquisition and technical characteristics of this requirement
- Industry's input and suggestions that would help refine and improve the Government's technical, acquisition, and management approaches

2. TECHNICAL CHARACTERISTICS:

DISA seeks information from respondents with cloud network and security integration experience. The chart below is a list of experience needed, in the following areas:

Secure Access Service Edge (SASE)
Direct to cloud traffic routing
Secure connection of users and devices to applications from various locations/networks
Integration with Zero Trust
Enterprise identity, federated identity sourcing,
Enterprise authentication methods, certificate-based authentication methods that continuously challenge user identity
Public key infrastructure
Geolocation analysis
User behavior analysis
Privileged access management
Role-based user access controls
Attribute-based user access controls
Conditions (events, signals, telemetry)-based access controls to users
Analytics and automation
Endpoint health & compliance
Security posture of devices as it relates to compliance such as implementation of STIGs, patch level, OS, applications, tools or agents missing, unauthorized software, qualified domain name, IP address, MAC address
Identifying suspicious endpoint behavior
Micro and macro-segmentation
Migrating security policies and rules amongst hosting environments
Data generation that is aligned to the DoD Data Reference Architecture
Automated tagging of data
Machine learning (ML) in support of tagging, analysis and authorization activities
Confidence level scoring in dynamic policy creation
Artificial intelligence (AI) for analysis of data in the creation of confidence levels.
Analyzed data decisions in the use of automated workflows through orchestration
Near real-time security decisions in automated tasks to update enforcement points
Integration with SD-WAN
Orchestrator clustering
Controller clustering
Virtual Edge Device support
Tunnel Support
Overlay Network
Peering Network
Hybrid Network (Overlay + peering + cloud)
SD-WAN Edge Endpoints
Orchestrator/Controller that is vendor managed and self-managed
Multi-tenancy
High Availability and COOP
Control Plane Loss Detection
Control Plane HA
Edge Device Loss Detection
Data Plane (Edge Device) HA
Data Plane COOP with Loss to Control Plane
Path Conditioning
Routing
Encryption
Native cloud integration
Cloud service integration
Key management and infrastructure

3. REQUESTED INFORMATION:
All requested information is intended to facilitate the Government's market intelligence efforts and inform the Government's acquisition approach.

4. CONTRACTOR PARTICIPATION:
Zero non-Government personnel will be used in the evaluation of RFI responses.

RESPONSE GUIDELINES:
Interested parties are requested to reply to this RFI **with a Response in accordance with the RFI Response Format provided in Appendix 1. Submissions shall not exceed one (1) page for the table with the requested vendor demographic information, two (2) pages for the response to Acquisition questions, four (4) pages for the response to Technical Capability questions, one (1) page for additional recommendations, and one page for the OCCI statement**. Submissions should be single spaced, 11-point type with at least one- inch margins on 8 1/2" X 11" page size. Cover pages are not included in the page limit. The response should not exceed a 5 MB e-mail limit for all items associated with the RFI response. Responses must specifically describe the contractor's ability to meet the requirements of this effort. Oral communications are not permissible. Companies who wish to respond to this RFI should send responses via email no later than ~~**14 June 2021**~~ **21 June 2021 at 8:00am EST** to Vanessa McCollum, Agreements Officer, at vanessa.a.mccollum.civ@mail.mil, Yolanda Dixon, Agreements Specialist, at yolanda.r.dixon2.civ@mail.mil, and the OTA Requirements mailbox address at disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil.

QUESTIONS:
Questions regarding this announcement shall be submitted in writing by email to Vanessa McCollum, Agreements Officer, at vanessa.a.mccollum.civ@mail.mil, Yolanda Dixon, Agreements Specialist, at yolanda.r.dixon2.civ@mail.mil, and the OTA Requirements mailbox at disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil. Verbal questions will NOT be accepted. Answers to questions will be posted to SAM.gov and DreamPort.net. All questions related to this RFI shall be received by **09 June 2021 at 5:00pm EST. Any questions received after the cut off date will not be answered.**

DISCLAIMER:
This RFI is not an RFPP and is not to be construed as a commitment by the Government to issue a solicitation or ultimately award a contract or agreement. Responses will not be considered as proposals nor will any award be made as a result of this synopsis. All information contained in the RFI is preliminary as well as subject to modification and is in no way binding on the Government. The Government will not reimburse companies for any costs associated with the submissions of their responses. Responders to this invitation are solely responsible for all expenses associated with responding to this RFI. This RFI will be the basis for collecting information on capabilities available. This RFI is issued solely for information and planning purposes.
Proprietary information and trade secrets, if any, must be clearly marked on all materials. All information received in this RFI that is marked "Proprietary" will be protected and limited in review to only those necessary in evaluating the proposal. Please be advised that all submissions become Government property and will not be returned nor will receipt be confirmed. Responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract or agreement.

Appendix 1: Request for Information (RFI) Response Format

1.0 Vendor Information (1 Page Max)

Provide the following Company information in the same format as the table below.

Company Name	
Company Address	
Point of Contact (Primary)	
Phone Number	
E-mail Address	
Cage Code	
DUNS	
Suggested NAICS	541511 (projected) Others applicable or suggested?
Company Web Page	
Other Classifications (e.g. large business, small business, SDB, HUBZone, 8(a), SDVOSB, WOSB, etc.)	
List Government Wide, DOD, or DISA contracts you are on that are applicable as a Prime or a Subcontractor (Includes partnering on Platform 1)	
Interest in this Acquisition as a Prime, Subcontractor, Teaming Arrangement, etc.	

2.0 Acquisition Strategy Questions (2 Page Limit)

2.1 Other Transaction Authority (OTA) and Challenge-Based Acquisition (ChBA)

Please provide feedback on the Government's proposed acquisition strategy, including the use of OTAs and ChBA.

2.2 Compliance with United States Code (USC) Title 10 Section 2371b(d)

Please describe your approach to satisfying USC Title 10 Section 2371b(d) applicability for OT authority. Describe whether your company qualifies as a non-traditional defense contractor and/or your approach for including nontraditional defense contractors, including small businesses, and/or implementing cost sharing.

2.3 Other Acquisition Strategy Recommendations

Please provide other relevant information regarding the Acquisition Strategy for this procurement.

3.0 Technical Capability Questions (4 Page Limit)

~~3.1 Communication Interface Management~~

~~*Please explain your company's experience and ability to manage interfaces between commercial and military communication systems. Specifically, describe approaches to ensure near-real-time access and data exchanges between IL-2, IL-5, and IL-6.*~~

~~3.2 CI/CD Strategy/Approach~~

~~*Provide a description of your approach to managing the CI/CD process for this system.*~~

~~3.3 Agile Framework and Methodology~~

~~*Specifically, how this Agile Framework can utilize short sprints, and how you would build to a Minimum Viable Product (MVP) and then continue that development to a Minimum Viable Capability Release (MVCR)*~~

~~3.4 How Automated Testing is Utilized in the Development Process~~

~~*Provide a basic description of your approach to implementing and utilizing automated testing techniques.*~~

~~3.5 A Potential User Feedback System~~

~~*How would User Feedback be collected and integrated into the development cycle.*~~

~~3.6 Product Backlog Management~~

~~*Provide any other corporate information relevant to this requirement.*~~

~~3.7 Management of Cloud Infrastructure and Infrastructure Costs~~

~~*Cloud Infrastructure costs will fluctuate throughout the life of this development, describe your approach to ensure that there is access to both growth and reduction in Cloud facilities as necessary.*~~

~~3.8 Processes, Tools, Documentation to Enable Continuous Development~~

~~*Describe your approach to ensuring that Continuous Development is both possible and efficiently performed.*~~

~~3.9 Suggested Program Office Integration~~

~~*Provide a description of your approach to ensuring there is clear communication with the Government Program Office and to ensuring the Government has sufficient access to development tools for monitoring*~~.

3.1 *Please explain your company's approach and innovations to creating, designing, developing and integrating SASE*

3.2 *Please explain your company's approach and innovations to creating, designing, developing and integrating Customer Edge Security Stacks at the DISN Point of Presence*

3.3 *Please explain your company's approach and innovations to creating, designing, developing and integrating scalable Application Security Stacks in front of application workloads*

3.4 *Please explain your company's approach and innovations to creating, designing, developing and integrating SD-WAS, including providing micro-segmentation and traffic flow prioritization*

3.5 *Please explain your company's approach and innovations to integrating capabilities with existing DISA capabilities at the NIPR (IL-4, 5) levels, and describe how your company would begin to implement new capabilities at the SIPR (IL-6) level.*

4.0 Recommendations (4 Page Limit)

Provide ~~any other~~ recommended acquisition or technical approaches that the Government should consider for this effort. Please refer to the technical characteristics in section 2 (page 2-3).

5.0 Organizational And Consultant Conflicts Of Interest (OCCI)

Each vendor shall specifically identify whether or not any potential or actual Organizational and Consultant Conflicts of Interest (OCCI) may exist for this potential OTA. If a vendor believes that an actual or perceived OCCI may exist on this procurement, the contractor shall, at this time, submit a statement that an OCCI may exist. If there are no OCCIs then the vendor shall submit an affirmative statement declaring that no OCCIs exist. DISA would like to remind companies deciding to pursue proposing on this potential OTA (in any prime, sub-vendor, or teaming arrangement capacity of their responsibility) to ensure they identify, proclaim, or declare, and take steps to avoid and/or mitigate, any potential OCCI issues. This is especially important for vendors supporting Government entities that may be involved in providing support activities for this effort.

6.0 Price (No Page Limit)

Provide Rough Order of Magnitude (ROM) and ROM narrative discussing the approach used to estimate the price of accomplishing all requirements. The Vendor shall assume the Government knows nothing about its capabilities or estimating approach.

At a minimum, the ROM narrative shall include the following cost categories for the ROM:

- *Labor: The ROM Narrative shall include the basis for which the estimate labor was calculated. i.e., Generic position titles and estimated rates and hours for those individuals).*

- *Material/Equipment: Provide a list of the materials/equipment required to meet the technical approach as described in the White Paper and the estimated cost.*

- *ODCs/Travel: Provide a list of the other direct costs required to meet the technical approach as described in the White Paper and the estimated costs with basis.*