



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency



Other Transaction Authority (OTA) Request for White Papers (RWP)

Project Number	DISA-OTA-21-9-Thunderdome
RWP Title	Thunderdome Zero Trust Solution
Issued by	Defense Information Systems Agency (DISA) Other Transaction (OT) Agreement Team www.DISA.mil
White Papers Due Date/Time (Suspense)	7 September 2021 / 1200 EDT 3 September 2021 / 1600 EDT 30 August 2021 / 0900EDT
Submit White Papers To	disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil vanessa.a.mccollum.civ@mail.mil tina.m.aviles,civ@mail.mil

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Amendment 0008 is issued to provide clarification on the FEDRAMP and IL4-6 in Section 3.4.2 and change the due date for submission of White Papers from September 3, 2021 at 1600 EDT to September 7, 2021 at 1200 EDT. The Government will not accept any further questions nor will it grant any additional extensions. All changes are highlighted in Red.

Amendment 0007 is issued due to administrative corrections to RWP Section 3.4.1 to correct numbering, update Section 2.2 Minimum Acceptability, Section 3.4.5. Price, and Section 6 to correct the RWP due date time from September 3, 2021 at 0900 EDT to September 3, 2021 at 1600 EDT. All changes are highlighted in Purple.

Amendment 0006 is issued to remove the Milestone Chart in RWP Section 3.4.4 (page 14) and amend RWP 3.4.1 to indicate offerors must submit a Milestone Chart. The RWP due date of September 3, 2021, at 1600 EDT remains unchanged. All changes are highlighted in Green.

Amendment 0005 is issued to provide responses to remaining vendor questions; amend RWP Sections 1.1, 3.4.1, 3.4.2, and 3.4.7; correct the Milestone Chart, and attach the Thunderdome Pilot Use Cases to RWP Amendment 0005. All changes are highlighted in Magenta.

Amendment 0004 is issued to respond to questions received by vendors, change the due date for submission of White Papers from August 30, 2021 to September 3, 2021, increase the page limit to twenty-five (25) pages, update section 2.1 Formatting to identify which attachments do not count towards the page limit, remove the reference to S-DNS, adjust the ROM template language, and revise the Milestone Chart. All changes are highlighted in teal.

Amendment 0003 is issued to respond to questions received during the Industry Q&A Session held on July 26, 2021, remove Ms. Yolanda Dixon from the Thunderdome effort and revise the RWP in response to Vendor questions. The following RWP Sections have been amended: 3.4.1, 3.4.2, 3.4.2d, 5.5, and 6. Section 2.5 has been added. Additionally, a vendor list to assist with teaming/partnering/subcontracting is attached. All changes are highlighted in yellow.

Amendment 0002 is issued to include Data Analytics requirements to Thunderdome in Section 3.4.1, update the purpose in Section 1.1, update the Milestone Chart in Section 3.4.3, change the due date for questions from July 28, 2021 to August 4, 2021 and change the due date for submission of White Papers from August 16, 2021 to August 30, 2021. All changes are highlighted in yellow.

Amendment 0001 was issued to correct header on pages 2-31 and revise Section 3.4.5, Table 1-ROM Template.

Note: Please advise DISA as soon as possible via email at disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil if your organization intends to submit a White Paper to DISA in response to this RWP.

The Defense Information Systems Agency (DISA) Cybersecurity Directorate (ID), through the DISA Procurement Services Directorate (PSD), is seeking White Papers from our industry partners on a proposed solution for the Thunderdome Zero Trust Architecture (ZTA) and implementation.

The Government desires a new approach to deliver an initial, minimum viable product (MVP) for the architecture of a Secure Access Service Edge (SASE), Software Defined (SD) Wide Area

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Network (WAN) with Customer Edge and Application Security Stack prototypes within six months of award for 25.4 SD-WAN sites and 5,000 users. Improvement and operational implementation of these capabilities through the year 2025 are planned. DISA expects the performing vendor to play a critical role interacting with key stakeholders across DISA and the Fourth Estate.

SECTION 1 OVERVIEW/DESCRIPTION

1.1 PURPOSE

This Request for White Paper (RWP) is being issued to prototype, develop, and test activities associated with DISA's ZTA and implementation, called Thunderdome.

DISA is planning the procurement of tools/systems/capabilities, which will assist in deploying a zero trust security model with SASE capability, integrated SD-WAN technology, Customer Edge Security Stacks, and Application Security Stacks on both the Secret Internet Protocol (IP) Router Network (SIPRNet) and Non-classified IP Router Network (NIPRNet).

The Government is planning on implementing key Zero Trust concepts within the SASE security framework. These are new operational capabilities for the Department of Defense (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 create, design, develop, and demonstrate the operational utility of SASE, Customer Edge Security Stacks at the Defense Information System Network (DISN) Customer Edge Point of Presence (PoP), along with scalable Application Security Stacks deployed in front of one or more application workloads.

The Government is seeking a cyber analytic capability that will retain, correlate and help analyze data for the purpose of Defensive Cyber Operations in the cloud.

SD-WAN integration includes the ability to provide micro segmentation and the prioritization of specific traffic flows. These capabilities will integrate with existing DISA systems (e.g. ICAM, Comply to Connect, Endpoint systems, SIEM, data analytics platforms, etc.) to provide conditional access and policies to limit functionality based on user and endpoint attributes, and policies based on application and data tagging. DISA will provide troubleshooting for alerting on the backbone or for customer connections to support the interface to the SD-WAN environment. Troubleshooting of the customer connections and RMA are the local tenants responsibility.

1.2 STATEMENT OF NEED

While the current defense-in-depth architecture has protected DoD data from adversaries in the past by placing various security products at multiple tiered locations, it has created independent security architectures across NIPR and SIPR.

DISA's current network architecture could improve in the following areas:

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

- a. Ability to authenticate all users and devices simultaneously and continuously at various locations
- b. Prevent lateral adversary movement
- c. Leverage attributes about the user and endpoint in continuous authentication decisions.
- d. Improve user experience by limiting the number of tools and sensors that their traffic must traverse
- e. Fully integrate cyber capabilities from the end point to the data.

SECTION 2 GENERAL SUBMISSION REQUIREMENTS

2.1 FORMATTING

Vendors are solely responsible for all expenses associated with responding to this RWP. White Papers shall follow the format described below. Evaluation and selection of the White Papers will be completed based on criteria in Sections 3 and 4. Responding to this RWP does not obligate the Government for costs associated with responding to this notice nor guarantee an award. The Government reserves the right to cancel this requirement at no cost to the Government if the Government determines no White Papers satisfy the criteria contained in Section 3.4 and/or no funding becomes available.

Subject to the availability of funds, the DISA/Defense Information Technology Contracting Organization (DITCO) at Scott AFB, IL intends to competitively issue this effort as an Other Transaction Authority (OTA) Agreement in accordance with 10 U.S.C. 2371b. If an OTA is awarded from this subject request, the Agreement is not considered a procurement contract and therefore, not subject to the Federal Acquisition Regulation (FAR) in accordance with 10 U.S.C. §2371.

The following **White Paper** formatting requirements apply:

- Times New Roman 10 (or larger) single-spaced, single-sided, 21.6 x 27.9 cm (8.5 by 11 inches);
- Smaller type may be used in figures and tables, but must be clearly legible;
- Margins on all sides (top, bottom, left, and right) should be at least 2.5 cm (1 inch);
- **Page limit is twenty-five (25) pages, does not include cover sheet and the *Affirmation of Business Status Certification [not to exceed (NTE) 15 pages], Rough Order of Magnitude (ROM) Template and narrative, Intellectual Property Statement/Agreements/Disclosures, Conflict of Interest Statement, Business Viability, Reference Owner(s) Statement, Table 2 – Data Rights Assertion, Section 7 Implementation of Section 889(a)(1)(B), Table 3 – Participants, Table of Content, and acronym list;***
- *Italic Red* text with brackets borders (e.g. [*company name*]) indicated areas for entry of information by the vendor. Delete all italicized text, contained within brackets before submittal of the White Paper;
- Page limitations shall not be circumvented by including inserted text boxes/pop-ups or

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

internet links to additional information. Such inclusions are not acceptable and will not be considered as part of the response to the RWP; and

- **DO NOT SUBMIT ANY CLASSIFIED INFORMATION.**

A White Paper **Cover Sheet** is required for all submissions and must include the following:

- OTA Project Number;
- Project Title;
- Company Title/Name of Proposed Solution;
- Date of Submittal;
- Primary point of contact (POC), including name, address, phone and e-mail contact information;
- Total ROM cost for the six month period of performance; and
- Disclosure of Information Statement (section 5.2).

2.2 MINIMUM ACCEPTABILITY

The Government will evaluate RWP submissions that are deemed as “complete”. To be considered “complete” submissions must contain, at a minimum, the following:

- Cover Sheet (section 2.1);
- Signed Intellectual Property Statements / Agreements / Disclosures (section 2.3);
- Signed Affirmation of Business Statement (section 2.4);
- Address all of the Evaluation Criteria Factors (sub-sections 3.4.1– 3.4.7).
- Rough Order of Magnitude for Proposed Solution
- **Milestone Chart**

If the vendor fails to include/address the minimum acceptability requirements (as defined above and throughout the RWP) the White Paper submission will/may be deemed non-compliant and inadequate for further evaluation.

2.3 INTELLECTUAL PROPERTY STATEMENT/AGREEMENTS/DISCLOSURES

2.3.1 SUBMITTER STATEMENT

Each participant shall complete the submitter statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

I, *[insert submitter’s full name]*, of *[insert full postal address]*, do hereby declare that the prototype that I have submitted, known as *[insert name of prototype]*, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that *[check one]*:

I do not hold and do not intend to hold any patent or patent application with a claim which may cover the prototype that I have submitted, known as *[insert name of prototype]*;

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

OR *[check one or both of the following]:*

to the best of my knowledge, the practice of the prototype that I have submitted, known as *[insert name of prototype]*, may be covered by the following U.S. and/or foreign patents: *[describe and enumerate or state “none” if applicable];*

I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted prototype *[describe and enumerate or state “none” if applicable].*

I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications, which may cover my prototype.

I do hereby agree to provide the statements required by Section 2.3.2 and 2.3.3, below, for any patent or patent application identified to cover the practice of my prototype and the right to use such for the purposes of the evaluation process.

Signature (electronic signature is acceptable)	✕ _____
Name	<i>[Insert Name of Representative]</i>
Title	<i>[Insert Title of Representative]</i>
Date	<i>[Insert Date of Signature]</i>

2.3.2 PATENT OWNER(S) STATEMENT

Each participant shall complete the Patent Owner(s) statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner’s authorized representative, of each patent and patent application identified.

I, *[insert full name]*, of *[insert full postal address]*, am the owner or authorized representative of the owner *[print full name, if different than the signer]* of the following patent(s) and/or patent application(s): *[enumerate]*, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the prototype known as *[insert name of prototype]* is selected for the DoD prototype, in consideration of its evaluation and selection, a non-exclusive license for the purpose of implementing prototype *[check one]:*

without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination,

OR

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

under reasonable terms and conditions (identified in section 3.4.6 –Proposed Data Rights Assertion) that are demonstrably free of any unfair discrimination.

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of evaluating the proposed prototype. Any future follow-on Production Contract or Agreement could/will require re-negotiated terms and conditions.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the evaluation process, and during the lifetime of the standard, a nonexclusive, non-transferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted prototype’s specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the prototype efforts.

Signature (electronic signature is acceptable)	✕
Name	<i>[Insert Name of Representative]</i>
Title	<i>[Insert Title of Representative]</i>
Date	<i>[Insert Date of Signature]</i>

2.3.3 REFERENCE OWNER(S) STATEMENT

Each participant shall complete the Reference Statement below. The statement shall be included as an attachment to the White Paper and will not count toward the page limit.

I, *[insert full name]*, *[insert full postal address]*, am the owner or authorized representative of the owner *[insert full name, if different than the signer]* of the submitted reference prototype’s specifications and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the evaluation process, and if the corresponding prototype is selected for a DoD prototype, notwithstanding that the implementations may be copyrighted or copyrightable.

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Signature (electronic signature is acceptable)	× _____
Name	<i>[Insert Name of Representative]</i>
Title	<i>[Insert Title of Representative]</i>
Date	<i>[Insert Date of Signature]</i>

2.4 AFFIRMATION OF BUSINESS STATUS CERTIFICATION

Each participant shall complete the certification below. The certification shall be included as an attachment to the White Paper and will not count toward the page limit. Please note that some sections in the certification may be left blank due to the type of business completing this form (e.g. non-traditional defense contractor).

Please note that in order to be eligible to submit a response to the Request for White Paper (RWP), vendors must meet the requirements outlined in 10 U.S.C Section 2371b(d)(1). As such, if a traditional defense contractor does not have a nontraditional defense contractor/nonprofit research institution/ small business participating to a significant extent in this prototype effort, then a traditional defense contractor **must** address how they will provide the one-third cost share to the Government. Vendors shall explain in their White Paper submission, NTE 15 pages, how they will meet these statutory requirements. Failure to provide the required explanation may result in your White Paper not being considered for this OTA effort.

Participant Name	<i>[Insert Participant Name]</i>
Proposed North American Industry Classification System (NAICS) Code	<i>[Insert NAICS Code]</i>
Industry Size Standard	<i>[Check one of the following boxes]</i> <input type="checkbox"/> Small <input type="checkbox"/> Large <input type="checkbox"/> Federally Funded Research & Development Center
Data Universal Numbering Systems (DUNS) Number	<i>[Insert DUNS Number]</i>
Commercial & Government Entity (CAGE) Code	<i>[Insert CAGE Code]</i>
Active System for Award Management (SAM) Registration	<i>[Check one of the following boxes and insert date]</i> <input type="checkbox"/> Yes <input type="checkbox"/> No Expiration Date:
Address 1	<i>[Insert Address Number and Street]</i>
Address 2	<i>[Insert suite, office, etc. Number]</i>
City/State/Zip Code	<i>[Insert City, State, Zip Code]</i>

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Point of Contact (POC) Name/Title	<i>[Insert POC Name and Title]</i>
POC Phone/Email	<i>[Insert POC Phone and Email]</i>

[Check one of the following boxes:]

Nontraditional Defense Contractor (NDC): A NDC is an entity that is not currently performing and has not performed, for at least the one-year period preceding the issuance of this Request for White Papers by the DoD, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 of the U.S. Code and the regulations implementing such section. All small businesses are considered NDCs. A small business is a business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632). To be considered a small business for the purposes of this RWP, a concern must qualify as a small business under the size standard for the North American Industry Classification System (NAICS) code, as described at 13 C.F.R. 121.201 and the proposed NAICS code above.

Traditional Defense Contractor: A traditional defense contractor is an entity that does not meet the definition of a NDC. Any traditional defense contractors must comply with 10 U.S.C Section 2371b(d)(1)(C) in order to be eligible to submit an RWP. As such, if a traditional defense contractor does not have a nontraditional defense contractor/nonprofit research institution/ small business participating to a significant extent in this prototype effort, then a traditional defense contractor **must** address how they will provide the one-third cost share to the Government.

This is to certify that the above is accurate, complete, and current as of *[MM/DD/YYYY]* for DISA-OTA-21-R-Thunderdome.

Signature (electronic signature is acceptable)	✕
Name	<i>[Insert Name of Representative]</i>
Title	<i>[Insert Title of Representative]</i>
Date	<i>[Insert Date of Signature]</i>

2.5 CONFLICT OF INTEREST (COI)

Each vendor shall specifically state in the white paper, whether there are any potential or actual conflicts of interest (COI) involving this OTA. If a vendor identifies a potential or actual COI, then the vendor shall submit a statement with the white paper explaining how the COI will be mitigated and/or avoided.

SECTION 3 EVALUATION APPROACH

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

The Government will employ a three-phased evaluation approach for the award of the Thunderdome prototype OTA. An award may be made to the responsible vendor whose offer, conforming to the requirements outlined in the RWP, is determined to be the best overall value to the Government, price, and other factors considered. The evaluation criteria are outlined in sub section 3.4.1 – 3.4.7.

Throughout the evaluation, the Government reserves the right, but is not obligated, to ask questions about individual vendor solutions. However, any response to the RWP that does not fully address all of requirements will be/can be eliminated from further consideration. This RWP constitutes Phase I of the evaluation, described below.

3.1 PHASE I – WHITE PAPER EVALUATION

The Government will conduct an evaluation of the White Paper(s) submitted in response to this RWP, in accordance with the evaluation criteria outlined in subsection 3.4.1 through 3.4.7. The White Papers will be evaluated to identify minimum viable products. Final selection(s) recommendation(s) will be made by the program management technical lead to the Agreements Officer (AO). After the evaluation of White Paper(s), the Government may select a solution and proceed to the next phase. Any vendor whose solution is not selected will be provided a letter containing notification of non-selection. OTAs are not subject to the FAR; therefore, the Agency will not provide feedback, which amounts to a debriefing.

3.2 PHASE II – ORAL PRESENTATIONS

The Government will invite selected vendor(s) from Phase I to provide oral presentations, which can be conducted in person, via videoconference, or phone. During the presentation, a vendor should be prepared to discuss, in detail, its solution. After the presentation, the Government will conduct evaluations and determine whether the vendor will proceed to the next phase. Any vendor whose solution is not selected will be provided a letter containing notification of non-selection. OTAs are not subject to the FAR; therefore, the Agency will not provide feedback, which amounts to a debriefing.

3.3 PHASE III – REQUEST FOR PROJECT PROPOSAL

The Government will issue a Request for Project Proposal (RFPP) to no more than two vendors from Phase II – Oral Presentations. The Government will provide an initial model OT to the selected vendor(s), which will be the Government’s opening position for negotiations. Using a collaborative process, the Government and each selected vendor will proceed to develop a detailed Project Work Statement and agree on milestones, KPPs, Terms and Conditions, and deliverables. These activities will be conducted separately for each vendor.

The Government will perform an evaluation of the final Project Proposals to ensure they meet the requirements and then proceed with award based on availability of funding. At the conclusion of Phase III, the Government intends to award one prototype OTA. In the event that the Government is unable to reach an agreement with the initial selectee, the Government may

negotiate with the other vendor invited to submit a Project proposal or may reevaluate Oral Presentation results and make another selection. The vendor whose solution is not selected will be provided a letter with brief explanation for non-selection. In the event that the Government is unable to reach an agreement with either RFPP recipient, the Government may re-evaluate Oral Presentation outcomes to make another selection.

3.4 EVALUATION CRITERIA

The overall evaluation will be based on the integrated assessment of the criteria outlined in sub-sections 3.4.1 – 3.4.7.

VENDORS ARE REQUIRED TO MEET ALL OF THE EVALUATION REQUIREMENTS, OBJECTIVES, AND REPRESENTATIONS. FAILURE TO RESPOND TO ANY OF THE FOLLOW EVALUATION FACTORS LISTED BELOW (SUB-SECTIONS 3.4.1 – 3.4.7) MAY RESULT IN ELIMINATION FROM CONSIDERATION.

3.4.1 TECHNICAL

The Government will evaluate the vendor's technical merit based on the criteria listed below:

- a. The vendor's approach creating, designing, developing and integrating SASE.
- b. The vendor's approach to implementing a SASE capability that can be managed by DISA as the Service Provider
- c. The vendor's approach to implementing a SASE capability that supports multitenancy (multiple customers and organizations)
- d. The vendor's technical approach to providing a proposed SASE solution that can be deployed to an on-premises customer location or a cloud-hosted enterprise location.
- e. The vendor's approach to creating, designing, developing and integrating Customer Edge Security Stacks at the DISN Point of Presence.
- f. The vendor's approach and innovations to creating, designing, developing and integrating scalable Application Security Stacks in front of application workloads.
- g. The vendor's approach to designing, developing and integrating Cyber Situational Awareness (SA) tools for Defensive Cyber Operations (DCO) and continuous monitoring
- h. The vendor's approach to ingesting, enriching, formatting and transforming data
- i. The vendor's approach to persisting data (90 days hot, 180 days warm, 365 days cold storage)
- j. The vendor's approach to querying, sharing and visualizing data for Cyber SA
- k. The vendor's approach to developing a Cyber SA solution that is portable and cloud agnostic to the greatest extent possible given the environment.
- l. The vendor's approach to standardized identity to authenticate users and devices
- m. The vendor's approach to developing new risk-based security policy to facilitate conditional access
- n. The vendor's approach to associate access policy to user attributes and device hardening status
- o. The vendor's approach to integrate endpoint technologies
- p. The vendor's approach to enable a wide range of devices and conditional access from diversified locations

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

- q. The vendor's approach to provide a consistent experience, optimized for the user's device, from any location on any device.
- r. The vendor's approach to deliver telemetry (logs/event data) in a continuous, consistent and low latency manner.
- s. ~~The vendor's approach to integrating with a secure DNS architecture.~~
- t. The vendor's approach to protecting DoD from distributed denial of service attacks
- u. The vendor's approach to ensure DISA will be able to support default (static route) or Border Gateway Protocol (BGP) peering from the SD-WAN controller to the DISN backbone on both NIPR and SIPR connections.
- v. The vendor's approach to provide tenant customers with a Service Portal providing service status and SLA metrics as well as the ability for tenant administrators to manage tenant-specific network and security service policies and configurations.
- w. The vendor's approach to automate and orchestrate the design and deployment of network and security services including the agile deployment of software enhancements, updates and patches.
- x. The vendor's approach to providing device inventory, software inventory, configuration, configuration compliance and vulnerability status, including the configurations of endpoint protection tools and capabilities.
- y. The vendor's approach and innovations to creating, designing, developing and integrating SD-WAN, including providing micro-segmentation, automated provisioning, and traffic flow prioritization.
- z. The vendor's approach for SD-WAN supporting user specified boundaries not limited by facility, geography, device, and warfighter movement and location.
- aa. The vendor's approach for SD-WAN using existing broadband capabilities – no Multiprotocol Label Switching (MPLS)/Virtual Local Area Networks (VLAN)
- bb. The vendor's approach to authenticating network flows before processing
- cc. The vendor's approach to encrypting network flows before transmission
- dd. The vendor's approach for SD-WAN for hybrid networking where some traffic is on SD-WAN and other traffic is on MPLS and over the top (OOT) operation
- ee. The vendor's approach to providing on-demand scalability of network and network paths when SLAs drop below user specified levels
- ff. The vendor's approach to monitoring SD-WAN and providing visibility into network traffic at a granular level
- gg. The vendor's approach to implementing the full solution at 4 NIPR sites (DISA HQ, DISA PAC, DISA EUR and JSP), with an estimated 5000 users per site.
- hh. The vendor's approach to testing and implementation of the full Thunderdome prototype, starting from the date of award to completion within 6 months, shall be depicted via a milestone chart.

3.4.2. SECURITY

- a. The vendor's approach to integrating capabilities with existing DISA capabilities at the NIPR (IL-4, 5) levels is clear and sound.
- b. The vendor description on how they would begin to implement new capabilities at the SIPR (IL-6) level, to include a testable lab prototype in the vendor's development environment that mirrors a NIPR solution. Existing space, power, and servers will not be provided by the Government. The solution must be built and demonstrated in an air gapped environment
- c. The vendor's approach to providing an architecture that is DoD Public Key Infrastructure (PKI) compliant
- d. The vendor's system must be FedRamp certified for IL-4-6 hosted environments, or in the process of approval with date of anticipated certification completion. DISA is willing to consider alternative approaches to deployment topologies that most effectively balance risk with speed to capability. Any response that is not FEDRAMP and/or IL5/6 approved should state the solution's current status in the process and the date the plan is expected to become compliant. FEDRAMP – HIGH (IL4) is considered sufficient for components of the system that allow the User-to-

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Application TLS session to remain intact. Any component or system which breaks that TLS session for examination/processing is required to be IL5. If there is a solution that is not FedRamp'd due to security or privacy concerns, that should be stated as well, along with a written exception to policy from the government. However, this does not mean that such solution will be accepted without the required FedRamp certification.

- e. The vendor's approach to complying with the DoD Risk Management Framework (RMF) to: identify, track and mitigate risk; conduct vulnerability scans; implement the applicable DISA Security Technical Implementation Guides (STIG); and document compliance status to support continuous monitoring and an Authority to Operate (ATO). Any part of the prototype solution that is on-premise will be required to achieve a full ATO to be considered for the full implementation.
- f. For the duration of the pilot, and IATT or IATO would be acceptable.
- g. The vendor's ability to provide a solution with a minimum of TLS 1.2 with 2048 bit RSA or p-384 ECC encryption, which is needed to support network flows

3.4.3 BUSINESS VIABILITY

Business viability shall be included as an attachment to the White Paper and will not count toward the page limit. Please address whether the company has the technical capability and resources to effectively accomplish the work. The White Paper should also address the following:

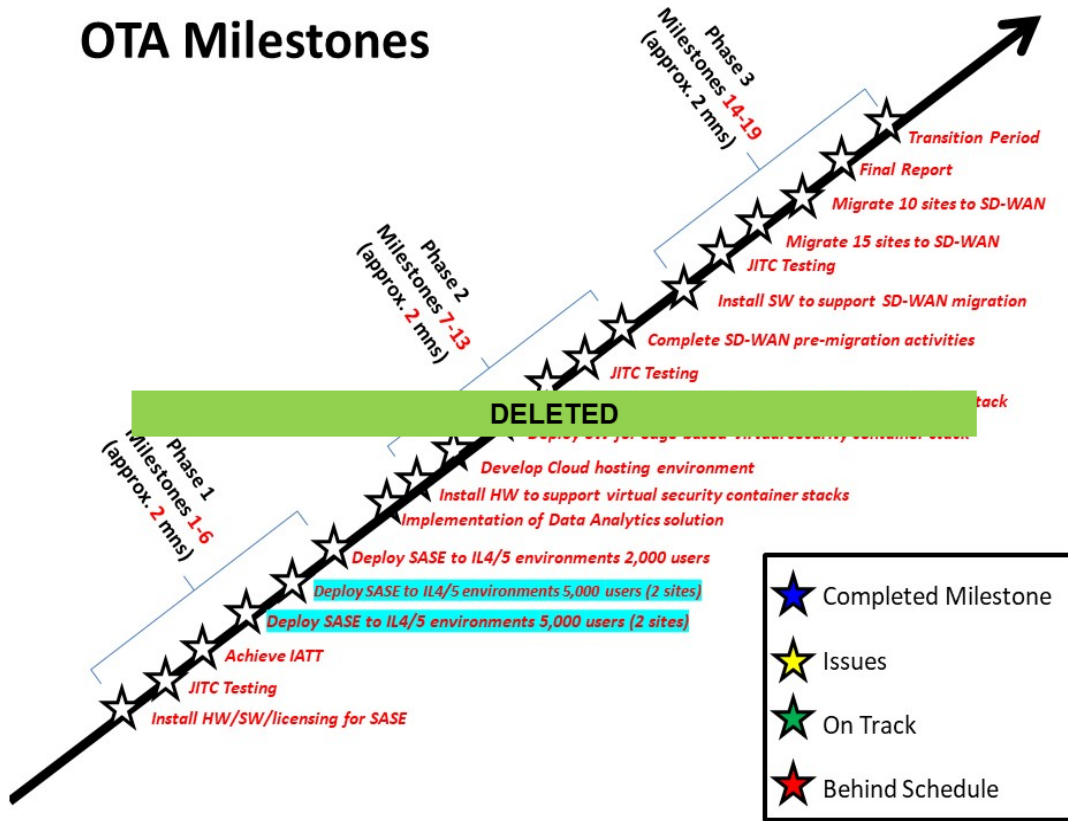
- a. Describe your company. How old is it? What are its core capabilities?
- b. Where is it located (e.g. multiple locations, sales/R&D in U.S. and other countries)?
- c. How many employees does your company employ?
- d. Describe the management team – who are your principals? What are their backgrounds and history?
- e. What is your annual revenue (sales and costs)?
- f. Will employees participating on project be U.S. citizens? If not, please identify employee name and country of origin.
- g. What is the main focus of your business?
- h. What are your firm's primary customers?
- i. What efforts similar in scope or complexity to the Thunderdome effort has your company successfully performed? Please provide specific details about similar projects.
- j. Do you have the personnel and resources necessary to perform this Agreement in house, or do you anticipate subcontracting some of the work? (If you expect to subcontract, in what area(s) do you expect to need third-party support, and why?)
- k. Where will the portion of the work to be accomplished at the Contractor's facilities be performed?

3.4.4 SCHEDULE

The Government will evaluate the vendors proposed schedule/timeline/sprints to include milestones, activities, and deliverables to research, evaluate, test, and deliver a prototype. The multifaceted concept exploration and design approach must demonstrate the vendors ability to meet the following schedule. The following deleted Milestone Chart was the Government's notional schedule only. Offerors are requested to revise the schedule as necessary based on

their innovative solution. The vendor shall submit a milestone chart with their White Paper depicting implementation of their proposed solution to be completed within six months from

OTA Milestones



award of the Prototype OTA.

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

3.4.5 PRICE

The vendor shall submit pricing data utilizing the Government's supplied Rough Order of Magnitude (ROM) Template (i.e., table 1). Failure to include the information described within this section may result in the vendor's entire Price/Cost criteria/factor being deemed non-compliant and inadequate for further evaluation review. **Table 1 is a ROM Template to assist vendors in submitting their ROM price breakdown. This template can be edited/milestones modified as deemed necessary for vendors to illustrate the total ROM cost of their proposed solution.**

In making a selection, the Government will consider affordability in comparison to the Government estimate to determine whether the proposed solution is in the best interest of the Government. The Government provided ROM Template (i.e., table 1) shall be included as an addendum or appendix to the White Paper and will not count toward the page limit. The vendor is responsible for verifying that the subtotals and totals within table 1 are correctly calculated.

The vendor ROM narrative shall discuss 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 also include the following cost categories for the ROM:

- **Prime Vendor Labor:** The ROM narrative shall include the basis for which the estimated labor was calculated. (i.e., Generic position titles and estimated rates and hours for those individuals). It is acceptable for the Vendor and Sub-vendor teams to work offsite; however, the Vendor team or integrator, should have a CAC-enabled team that has access to the DISA Headquarters.
- **Sub-Vendor/Consultant Labor:** Provide a list of sub-vendor/consultant effort required to meet the technical approach as described in the white paper and the estimated cost. Include the basis for which the estimated labor was calculated, (i.e., Generic position titles and estimated fully burdened hourly 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; The Vendor shall provide all hardware and software to support the Vendor's solution.
- **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; Identify any expenses incurred by an employee while those individuals are traveling for business purposes. (e.g., estimated costs for lodging, transportation, and meals) and identify the basis for how the travel costs were calculated.

The Government does not require supporting data to justify the estimated costs (e.g., copies of commercial/market price lists/rates, price history, subvendor quotes, invoices) with the submission of the White Paper. However, vendors will be required to supply the supporting data upon the Request for Project Proposal, if selected.

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

Table 1 – ROM Template

Element s	FY2022 (Six Months)
Phase 1 (Milestones 1-6)	
Prime Vendor Labor	<i>[Insert Total Cost for Prime Labor for Fiscal Year 2022]</i>
Sub – Vendor/Consultant Labor	<i>[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022]</i>
Material/Equipment	<i>[Insert Total Cost for Material/Equipment for Fiscal Year 2022]</i>
Other Direct Costs (ODCs)/Travel	<i>[Insert Total Cost for ODCs for Fiscal Year 2022]</i>
SUBTOTAL	<i>[Insert Total Cost for Phase 1 for Fiscal Year 2022]</i>
Phase 2 (Milestones 7-13)	
Prime Vendor Labor	<i>[Insert Total Cost for Prime Labor for Fiscal Year 2022]</i>
Sub – Vendor/Consultant Labor	<i>[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022]</i>
Material/Equipment	<i>[Insert Total Cost for Material/Equipment for Fiscal Year 2022]</i>
Other Direct Costs (ODCs)/Travel	<i>[Insert Total Cost for ODCs for Fiscal Year 2022]</i>
SUBTOTAL	<i>[Insert Total Cost for Phase 2 for Fiscal Year 2022]</i>
Phase 3 (Milestones 14-19)	
Prime Vendor Labor	<i>[Insert Total Cost for Prime Labor for Fiscal Year 2022]</i>
Sub – Vendor/Consultant Labor	<i>[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022]</i>
Material/Equipment	<i>[Insert Total Cost for Material/Equipment for Fiscal Year 2022]</i>
Other Direct Costs (ODCs)/Travel	<i>[Insert Total Cost for ODCs for Fiscal Year 2022]</i>
SUBTOTAL	<i>[Insert Total Cost for Phase 3 for Fiscal Year 2022]</i>
Total All Phases	
Prime Vendor Labor	<i>[Insert Total Cost for Prime Labor for Fiscal Year 2022]</i>
Sub – Vendor/Consultant Labor	<i>[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2022]</i>
Material/Equipment	<i>[Insert Total Cost for Material/Equipment for Fiscal Year 2022]</i>
Other Direct Costs (ODCs)/Travel	<i>[Insert Total Cost for ODCs for Fiscal Year 2022]</i>
TOTAL	<i>[Insert Total Cost of All Phases for Fiscal Year 2022]</i>

*Thunderdome
Request for White Papers
Project Number: DISA-OTA-21-9-Thunderdome*

3.4.6 DATA RIGHTS ASSERTION

State whether there are any data rights issues that the Government should be cognizant of moving forward. Specifically, please identify any intellectual property, patents and inventions involved in the proposed solution and associated restrictions on the Government’s use of that intellectual property, patents and inventions. The following table shall be presented for all assertions.

Table 2 – Data Rights Assertion

Technical Data/Computers Software/ Patent to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Entity Asserting Restrictions
<i>[Identify the technical data/software/patent to be furnished with restriction]</i>	<i>[Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government’s right should be restricted]</i>	<i>[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]</i>	<i>[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]</i>

3.4.7 PARTICIPANTS

List all participants (i.e. other vendors), including description of contributions and significance of each participant.

Should a potential offeror be selected to move into Phase II, Oral Presentations, offerors MUST advise the Government immediately when any changes to the participant list are anticipated. Additionally, the Government MUST receive an updated participant list no later than (NLT) two (2) business days prior to the scheduled presentation or the presentation may be canceled.

Table 3 – Participants

Participant	Business Status (Check one)	Participant Contribution and Significance to Overall Project
<i>[Insert separate row(s) for each additional participant. Delete row(s) as applicable if Participant is the only participant.]</i>	<input type="checkbox"/> Traditional <input type="checkbox"/> Non-Traditional	<i>[Insert detailed, quantifiable description which addresses the following:</i> <ul style="list-style-type: none"> • <i>What is this Participant’s significant contribution?</i> • <i>Why is this Participant’s contribution significant to the overall project?</i> • <i>How is this Participant uniquely qualified to provide this significant</i>

OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX

		<i>contribution? (Note: number of years of experience is not deemed a unique qualification.) [Failure to provide the required explanation may result in your White Paper not being considered for this OTA effort.]</i>
--	--	---

The facility(ies) where the proposed work is to be performed and the equipment or other Participant property which will be utilized for the prototype include: *[Insert a brief description of facility(ies)/equipment proposed for use on the project].*

SECTION 4 AWARD

4.1 SELECTION DECISION

It is the Government's intention to negotiate, select, and fund a Prototype Project at the conclusion of the three-phased evaluation approach, described in Section 3, which best meets the evaluation criteria listed in Sub-Section 3.4. The White Paper selection will be conducted in accordance with Government procedures and the evaluation criteria in Sub-Section 3.4. The Government will make a determination whether to:

- Select the White Paper(s), or some portion of the White Paper(s); or,
- Reject the White Paper(s) for further consideration.

The White Paper basis of selection decision will be formally communicated to vendors in writing. Once the selection of the best solution is made, the Government team may proceed to the next phase of the evaluation. At any time during evaluations, the Government may choose to cancel this requirement. In case of cancellation, the Government will not be responsible for any expenses associated with responding to this RWP.

4.2 FOLLOW ON PRODUCTION

The Government intends to award one (1) prototype OTA. Prior to awarding a prototype OTA, the Government will ensure that it is in compliance with 10 USC §2371b(d)(1). The Government will obtain approval from the appropriate approval authority, based on the dollar threshold projected for the prototype OTA. This will be done prior to entering into the prototype OTA with a selected vendor.

Provided that the prototype OTA is successfully completed, the Government may award a follow-on production FAR-based contract or OTA to the participant in the transaction for the prototype project, without further competition. **The Government will only take into production the same solution prototyped and determined successfully completed.** If it is determined that transition activities are in the best interest of the Government, then the Government reserves the right to bilaterally modify the Agreement by adding such activities. Prior to award of the production contract or

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

transaction, the Government will ensure that it complies with 10 USC 2371b(f). In addition, the Government will again obtain approval from the appropriate approval authority, based on the dollar threshold projected for the production FAR-based contract or production OTA.

SECTION 5 ADDITIONAL INFORMATION

5.1 DOCUMENTATION CLASSIFICATION

Vendors shall not submit any documentation that is classified as “Confidential,” “Secret,” or “Top Secret” throughout the evaluation process. This includes, but is not limited to submission of White Papers, Project Proposals, Project Work Statements (PWS), etc.

5.2 DISCLOSURE OF INFORMATION

White Papers, Project Proposals, PWS, etc. containing data that is not to be disclosed to the public for any purpose or used by the Government except for evaluation purposes shall include the following sentences on the cover page:

“This White Paper includes data that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is issued to this Company as a result of -- or in connection with -- the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent agreed upon by both parties in the resulting agreement. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets *[insert numbers or other identification of sheets]*.”

5.2.1 DATA SHEET MARKINGS

Marking requirements specify that data be “conspicuously and legibly” marked with a protective legend that identifies the OTA number, vendor’s name and address, and the submittal date, along with the warning “*Use or disclosure of data contained on this sheet is subject to restriction*” on the title page of any restricted data sheets.

5.3 ANALYTICAL AND LABORATORY STUDIES

It is generally desired that active research and development (R&D) is underway for concepts submitted under this effort. Active R&D includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology, as well as software engineering and development. The Government is requesting information on any current or ongoing analytical or laboratory studies related to the prototype solutions. Any information related to ongoing efforts shall be included as an attachment to the White Paper and will not count toward the page limit.

5.4 RECORDS, FILES, AND DOCUMENTATION

All physical records, files, documents and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this OTA, maintained by the vendor which are to be transferred or released to the Government, shall become and remain Government property and shall be maintained and disposed of as applicable. Nothing in this section alters the rights of the Government or the vendor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this RWP (including all clauses that are or shall be included or incorporated by reference into the prototype OTA). The AO may at any time issue a hold notification in writing to the vendor. At such time, the vendor may not dispose of any Government data or Government-related data described in the hold notification until such time as the vendor is notified in writing by the AO and shall preserve all such data IAW Agency instructions. The vendor shall provide the AO within ten (10) business days of receipt of any requests from a third party for Government-related data. When the Government is using a vendor's prototype solutions, the vendor shall provide the Agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

5.5 SECURITY CLEARANCES

The vendor is responsible for providing personnel with interim secret security clearances to ensure compliance with Government security regulations. **An Interim Secret security clearance will be required for all personnel involved with the prototype, beginning at time of award.** Clearances are not required for SME vendor. The vendor shall fully cooperate on all security checks and investigations by furnishing requested information to verify the vendor employee's eligibility for any required clearance.

The vendors proposed solution (e.g., data, integration with supporting DoD Infrastructure, architecture) will determine the personnel security clearance requirements for the prototype effort. The Government will provide additional details regarding the required security clearances in the RFPP.

5.6 DATA STORAGE

To protect against seizure and improper use by non-United States (U.S.) persons and government entities, all data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the U.S. The vendor will be required to maintain all government data that is not physically located on DoD premises within the 50 States, the District of Columbia, and outlying areas of the U.S., unless otherwise authorized by the responsible Government, as described in DoDI 8510.01 and the DoD Cloud Computing Security Requirements Guide. If the Government data is co-located with the non-Government data, the vendor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Agreements Officer, and without the vendor's involvement. The vendor shall record all

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

physical access to the cloud storage facilities and all logical access to the Government data. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Agreements Officer or designee in accordance with the agreement or upon request to comply with federal authorities.

5.7 LAW ENFORCEMENT

The vendor shall acknowledge and affirm that United States (U.S.) Federal law enforcement officials do not need a warrant or a subpoena to access Government data on any system or media employed by the vendor or their sub-vendors or other partners, or allies, to deliver or otherwise support the contracted service for the U.S. Government, subject to requirements for access to classified information and release thereof, if applicable. As specified by the Agreements Officer, the vendor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any vendor facility with Government data.

5.8 NOTIFICATION

The vendor shall notify the Government Security Contacts (Disa.meade.bd.mbx.sd-security-managers@mail.mil), and the AO within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The vendor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

5.9 VENDOR INCURRED EVALUATION COSTS

The costs associated with participating in and responding to Phases I through III, to include White Paper(s) preparation and submission, are not considered an allowable charges and should not be included within the ROM or any pricing information.

5.10 EXPORT CONTROLS

Research findings and technology developments arising from the resulting White Paper may constitute a significant enhancement to the national defense and to the economic vitality of the United States. As such, in the conduct of all work related to this effort, the recipient will comply strictly with the International Traffic in Arms Regulation (22 CFR 120-130), the National Industrial Security Program Operating Manual (DoD 5220.22-M) and the Department of Commerce Export Regulation (15 CFR 730-774).

SECTION 6 RESPONSES

The Government will host an Industry Question and Answer session on July 26, 2021. If

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

interested in participating, please submit contact information for up to four company personnel to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Agreements Officer at vanessa.a.mccollum.civ@mail.mil and Agreements Specialist at tina.m.aviles.civ@mail.mil no later than July 20, 2021 at 1600 Eastern Daylight Time (EDT).

Questions should be addressed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Agreements Officer at vanessa.a.mccollum.civ@mail.mil and Agreements Specialists at tina.m.aviles.civ@mail.mil. Please provide any questions, in writing, no later than ~~July 28, 2021~~ **August 4, 2021** at 1600 EDT. Responses to vendor questions will be provided in amendments to the RWP. The Government reserves the right to not answer questions submitted after this time. Any submissions that are received after the close of the solicitation period will receive no further consideration.

The response shall be due no later than ~~August 16, 2021~~ **August 30, 2021** ~~September 3, 2021~~ **September 7, 2021** at ~~1200~~ **1600** ~~0900~~ EDT. The responses shall be emailed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Agreements Officer at vanessa.a.mccollum.civ@mail.mil and Agreement Specialist at tina.m.aviles.civ@mail.mil.

SECTION 7 IMPLEMENTATION OF SECTION 889(A)(1)(B) OF THE JOHN S. MCCAIN NATIONAL DEFENSE AUTHORIZATION ACT (NDAA) FOR FISCAL YEAR 2019

REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

The offeror shall not complete the representation at paragraph (d)(1) of this provision if the offeror has represented that it “does not provide covered telecommunications equipment or services as a part of its offered Products or services to the Government in the performance of any contract, subcontract, or other contractual instrument” in the provision at 52.204-26, covered telecommunications equipment or services—Representation, or in paragraph (v) of the provision at 52.212-3, offeror Representations and Certifications-Commercial Items.

(a) Definitions. As used in this provision—

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on contracting for Certain Telecommunications and Video Surveillance Services or equipment.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as

OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX

part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or

services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The offeror shall review the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

(d) Representation. The offeror represents that—

(1) It will, will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the offeror responds “will” in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the offeror represents that—

It does, does not use covered telecommunications equipment or services, or use

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

any equipment, system, or service that uses covered telecommunications equipment or services. The offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the offeror responds “does” in paragraph (d)(2) of this section.

(e) Disclosures.

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the offeror has responded “will” in the representation in paragraph (d)(1) of this provision, the offeror shall provide the following information as part of the Offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the offeror has responded “does” in the representation in paragraph (d)(2) of this provision, the offeror shall provide the following information as part of the Offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology company, or Dahua Technology company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using

*OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX*

such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the Government of a Covered foreign country.

critical technology means—

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications

OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX

equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The vendor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain national defense authorization Act for fiscal year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit vendors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the vendor identifies covered telecommunications equipment or services used as

OTA Title
Request for White Papers
Project Number: DISA-OTA-XX-R-XXXX

a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the vendor is notified of such by a Subvendor at any tier or by any other source, the vendor shall report the information in paragraph (d)(2) of this clause to the contracting officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the vendor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the vendor shall report to the contracting officer for the indefinite delivery contract and the contracting officer(s) for any affected order or, in the case of the Department of Defense, identify both the

indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The vendor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the vendor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The vendor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.