Request for White Papers:
Cloud Based Internet Isolation (CBII)
Project Number: DISA-OTA-19-R-CBII

Section 1. Request for White Papers

1.1 Purpose

This Request for White Paper (RWP) is issued to seek Vendors capable of fulfilling the technical objectives outlined below related to CBII.

1.2 Statement of Need

DoD spends tens of millions of dollars in an effort to protect the networks from Internet born threats and attacks, approximately 36 percent of which are browser based. The implementation of the Cloud Based Internet Isolation capability, which has been used in the commercial sector to isolate Internet traffic, will mitigate the threats and free up the bandwidth capacity, by redirecting internet browsing from the end user's desktop into a remote cloud-based server. However, it has never been implemented at scale in any DoD entity or component. The successful implementation of this effort will directly enhance military and civilian personnel's ability to defend the Department of Defense Information Network (DODIN).

The project's objective is to prototype a limited scale (100,000 users) implementation of a Cloud Based Internet Isolation capability amongst two (2) vendors to refine processes and requirements necessary for large scale implementation across the DoD Enterprise. Deliverables include prototype architecture documents, analysis artifacts, incorporation of feedback from the user community into the final product, and the final report.

1.3 General Information

Vendors are solely responsible for all expenses associated with responding to this RWP. White Papers shall follow the format described in Section 2. Evaluation and selection of the white papers will be completed based on criteria in Sections 3 and 4. Funding for this project is currently unavailable. Responding to this Request for White Papers does not obligate the Government for costs associated with responding to this notice. The Government reserves the right to cancel this requirement if no White Papers satisfy the criteria contained in Section 3 and/or no funding becomes available to proceed to the Request for Final Proposal phase.

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

The following general 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 fifteen (15) pages, does not include cover and certification pages.
- Please note that page limitations shall not be circumvented by including inserted text boxes/pop-ups or internet links to additional information. Such inclusions are not acceptable and will not be considered as part of the response to Request for White Papers.
- **DO NOT SUBMIT ANY CLASSIFIED INFORMATION.**

White Papers shall include a cover sheet (not counted toward the page limit) that includes:

- Prototype Project title.

- Primary point of contact, including name, address, phone and e-mail contact information.
- Total Solution Rough Order of Magnitude (ROM) cost.
- Date of submission.

2.1 Technical Section Requirements

The technical section of the White Paper shall contain, as a minimum, the following:

- Background and Benefits of Proposed Solution
- Technical Approach, including clearly defined prototype solution
- Schedule and Deliverables

2.2 Price Section Requirements

The White Paper shall contain a ROM to illustrate the total price. The format for the ROM shall be provided in accordance with Section 3.1.5. The pricing strategy provided in the ROM submission will be used to determine if the White Paper Response is in the best interest of the Government.

2.3 Affirmation of Business Status Certification

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

Affirmation of Business Status Certification

Business Entity	
Proposed NAICS Code	
Industry Size Standard (Small / Large)	
DUNS No.	
CAGE Code	
Active SAM Registration	☐ **Yes** ☐ **No** **Expiration Date:**
Address 1	
Address 2	
City/State/Zip	
POC Name/Title	
POC phone/email	

☐ **Nontraditional Defense Contractor (NDC)** - A nontraditional defense contractor 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 Department of Defense, any contract or subcontract for the Department of Defense 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 nontraditional defense contractor (NDC).

This is to certify that the above is accurate, complete, and current as of _____ for DISA-OTA-19-R-CBII.

Signature	
Name	Angela D. Landress
Title	Program Manager
Date	

Section 3: Evaluation Approach

The evaluation will be conducted in three phases, as follows:

Phase I

The Government will conduct an evaluation of all eligible White Paper(s) submitted in response to this RWP. After the evaluation of White Paper(s), the Government will select solution(s) that will proceed to the next phase. Any vendor whose solution is not selected, will be provided a letter containing a brief explanation for non-selection.

Phase II

The Government will invite selected vendors to provide oral presentation, which can be conducted in person, via videoconference, or phone. During the presentation, a vendor should be prepared to discuss in detail its solution, which includes but is not limited to: (1) how the solution will be engineered; (2) how the vendor will use policy based routing, or proxies, to move a portion of the traffic over; (3) what kind of rules/policies vendor thinks need to be in place for successful implementation of the prototype solution; (4) how does a vendor propose to protect the cloud space from attacks; (5) how will the routers be protected; and (6) what is the cost and schedule proposed for the implementation of the solution. After the presentation, the Government will conduct evaluations. Any vendor, whose solution is not selected, will be provided a letter with brief explanation for non-selection.

Phase III

The Government will issue a Request for Project Proposals to the selected vendors. Vendors will then be invited to meet with the Government in order to engage in negotiations. The Government will provide an initial model OT Agreement to the selected vendors, which will be the Government's opening position for negotiations. Using a collaborative process, the Government and each vendor will develop a detailed Project Statement of Work, negotiate Terms and Conditions, agree on milestones and deliverables, and negotiate final price. The Government will perform an evaluation of the final Project Proposal to ensure it meets the requirements and then proceed with award based on availability of funding. At the conclusion of Phase III, the Government intends to award two prototype OTAs. In the event that the Government is unable to reach an agreement with the initial selectee(s), the Government may reevaluate White Paper Responses and make another selection(s).

3.1 Evaluation Criteria

The overall evaluation will be based on an integrated assessment of the below criteria:

1. Relevance

   The Government will determine whether vendor's submission is relevant to the posted RWP. Please note that if the submission is not relevant to the posted RWP, it will not be evaluated further.

2. Technical Merit

   Vendor's solution will be evaluated based on the criteria listed below.

   a. The Enterprise Cloud Based Internet Isolation capability shall consist of the (1) through (19) areas identified below. Please note that requirements in areas (20) through (23) are optional:

      (1) The ability to send either all or a configurable portion of user Internet activity at the browser to a Cloud-based vendor solution external to the DoDIN. All of the requirements in (i) through (ix) must be met:
         i. isolate all Internet code execution in the cloud
         ii. isolate each user's session
         iii. provide the ability to route internet browsing activity of Android and iOS mobile devices (not connected to DoDIN) via the solution
            1. Provide access via a proxy for mobile users that are not connected to the DoDIN
         iv. support Role-Based Access Control (RBAC) and grant system administrators access to configure as required by the user role
         v. support data encryption and encrypt the connection between the user endpoint and system host
         vi. browsing capability shall provide non-attribution such that no DoD metadata is visible to any third party
         vii. provide the ability to downgrade video and audio quality for streaming Internet media (configurable Quality of Service (QOS))
         viii. provide compression to limit bandwidth utilized in delivering rendering of isolated Cloud session back to the client workstation
         ix. provide the ability to timeout connections on inactive tabs after a configurable time limit

      (2) The solution shall securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

      (3) The system shall route file downloads through a DoD-specified security stack.

      (4) The solution shall include content control software at the host location to:
         i. scan documents for malicious code/infection before transmitting them to the DoDIN;

         ii. provide intrusion protection for persistent document storage commensurate with protections in the National Institute of Standards and Technology Special Publication 800-122 required for storing personally identifiable information;

         iii. allow blacklisting and whitelisting Uniform Resource Locator (URL)s by category, geolocation, and uncategorized URL blocking:
            1. provide for updating 'uncategorized' URL with categorization provided by user within 0-1 hour; and

2. provide the user the ability to update a blacklisted site to a whitelisted site if wrongly categorized within 0-1 hour; and

iv. allow and block file downloads/uploads by file type; allow to open downloaded files within the cloud session.

(5) The solution shall log all web requests and tie the web request to specific users from authentication through session end and be able to:
   i. Capture logs from content control software, blacklisting/whitelisting, data about downloaded files, logs based on geolocation and capture geolocation within the logs;
   ii. Log data can inform analysis and facilitate threat sharing with other systems such as Security Information and Event Management (SIEMs) and perimeter based defenses; and
   iii. Log files are separated by organization and secured appropriately.

(6) The solution shall have the ability to allow distinct groups to set thresholds for Internet usage on a per-client basis; send notification to the user if daily bandwidth threshold is within a configurable percentage of being met, has been met, has been exceeded; and send an automated e-mail to designated e-mail address(s) if threshold has been exceeded by a configurable amount.

(7) The solution shall provide non-repudiation of browser activity.

(8) The solution shall support all current and legacy web content technologies, such as Java, Flash, Silverlight, Hypertext Markup Language (HTML), Windows 10, mobile devices running DISA-supposed version of Android and iOS, and common web browsers (i.e., Internet Explorer, Firefox, Chrome, Edge, Safari).

(9) The solution shall support the ability to configure the user session inactivity timeout.

(10) The solution shall support the ability to resume a session after time out.

(11) The solution shall support connections to websites utilizing Secure Sockets Layer (SSL) 3.0 and Transport Layer Security (TLS) 1.0-1.3.

(12) The solution shall support DNS-over-TLS when available.

(13) The solution shall support Encrypted Server Name Indication (ESNI) when available.

(14) The solution shall meet the following performance criteria outlined in (i) through (vi) below as follows:
   i. be able to provide information near real-time;
   ii. support a start time from opening the client to the browsing session start of no more than 5 seconds;
   iii. offer a latency of no more than 100ms from the nearest DoDIN meetme router location to the service host;
   iv. support 10 Gigabits per second throughput minimally shall be available 99% of the time;
   v. support Recovery Time Objective of 0-1 hours; and
   vi. support browsing concurrent tabs of >25 without drop in configured QOS.

(15) The solution shall require users to authenticate to gain access:

i. The solution shall utilize DoD provided Directory service for user profiles; and
ii. The solution shall support DOD-PKI authentication either natively or via token from an authentication proxy.

(16) The vendor shall install and maintain 10G circuit between meetme router and cloud provider.

(17) The cloud service provider shall submit a supply chain risk management (SCRM) plan in accordance with FedRAMP security control SA-12.

(18) Vendor shall submit to protocol analysis of the traffic between the service and client.

(19) The system must be housed in data center(s) that are at a minimum FedRamp impact level II certified.

Please note that requirements identified in areas (20) through (23) are optional. Vendors are not required to propose a solution to meet the requirements in areas (20) through (23). However, if these requirements can be met as part of the vendor's solution, please briefly explain how they can be met.

(20) (Optional) The solution shall isolate URLs that are opened from email.
i. The solution shall provide the ability to view attachment files remotely in the isolation environment.

(21) (Optional) The solution shall provide anti-virus and heuristic analysis within the cloud environment to block malware from being downloaded into the DoD environment.

(22) (Optional) The solution shall provide a detonation chamber capability to allow execution of suspicious code prior to download.

(23) (Optional) The solution shall provide a data loss prevention capability natively within the solution.

3. Business Viability

Please address whether the company has the technical capability and resources to effectively accomplish the work.

4. Price:

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. Please note that any licenses fees that utilizes a per user cost model will not be acceptable for this effort. Any other licenses fees, that include, but are not limited to a 25% of 50,000 users concurrent user rate cost model, will be considered as acceptable.

This section shall include the ROM cost and ROM narrative associated with meeting the technical requirements as described in the White Paper. This shall include at a minimum the estimated costs for Labor, Material/Equipment, Other Direct Costs and Sub-contracts. Include the following table in this Section.

ROM	
Elements	Amount
Prime Contractor Labor	$-
Material/Equipment	$-
Other Direct Costs (ODC)	$-
Subcontractor/Consultant Labor	$-
Proposed Cost Share (if applicable)	$-
Total Solution ROM	$-
Optional Requirements from Paragraph 3.1.2b(19) – (22)	$-
TOTAL ROM	$-

The ROM Narrative shall include, at a minimum, details on the following cost categories for the ROM:

- Prime Labors. 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.
- ODC: Provide a list of the other costs (e.g., travel) required to meet the technical approach as described in the White Paper and the estimated cost.

Subcontractor/Consultant: Provide a list of subcontractor/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.)

The Government does not require supporting data to justify the estimated costs (e.g., copies of commercial/market price lists/rates, price history, subcontractor quotes, invoices) with the submission of the white paper. Vendors shall supply the supporting data upon the Request for Project Proposal.

5. Schedule

In this section, please provide an estimated timeline within which you expect to successfully complete the work.

6. Data Rights

In this section, please 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:

Technical Data/ Computer Software/ Patent to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Entity Asserting Restrictions

7. Participants

   In this section, please list all participants (i.e. other vendors), including description of contributions and significance of each participant.

Section 4. Basis for Selection
It is the Government's intention to negotiate, select and fund Prototype Project(s) at the conclusion of the three (3) phase approach, described in Section 3, that best meets the evaluation criteria listed in Sub-Section 3.1. The White Paper selection will be conducted in accordance with Government procedures and the evaluation criteria in Sub-Section 3.1. The Government will make a determination whether to:

a) Select the White Paper(s), or some portion of the White Paper(s);
b) Retain the White Paper(s) in a library for potential future requirements for three (3) years; or,
c) 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(s) is made, the Government team will proceed to Phase II and Phase III.

4.2 The Government intends to award two prototype OTA Agreements. Provided that the prototype OTA(s) is (are) successfully completed, the Government may award only **one** follow-on production contract or transaction to the participant in the transaction for the prototype project, without further competition. The scale of a production contract or transaction will encompass all users connected to the DoDIN, which is approximately 3.5 million users across the Department of Defense.

Section 5: Additional Information

5.1 Security Requirements

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, etc.

5.2 Other Special Requirements

5.2.1 It is generally desired that active 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.

5.2.2 The costs associated with participating in Phases I through III, to include white paper(s) preparation and submission, are **not** considered an allowable charge to any contract or agreement.

5.3 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).

5.4 Disclosure of Information

White papers, Project Proposals, Project Work Statements, 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]"

5.4.1 Each restricted data sheet should be marked as follows:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this white paper."

Section 6: Responses

The response shall be due no later than **4:00 PM** Central Standard Time (CST) on **7 December 2018**. The responses shall be emailed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, Ms. Vanessa McCollum, vanessa.a.mccollum.civ@mail.mil, Ms. Coni Jackson, constance.e.jackson.civ@mail.mil, and Mr. Kris Onstott, kristopher.j.onstott.civ@mail.mil.