Request for Information (RFI) for
Cloud Based Internet Isolation Solution

The Defense Information Systems Agency (DISA) Requirements and Analysis Office (RAO) is seeking information from industry to assist with the development and planning of a potential new requirement.

THIS IS A REQUEST FOR INFORMATION (RFI) NOTICE ONLY. THIS IS NOT A REQUEST FOR PROPOSALS (RFP). NO SOLICITATION IS AVAILABLE AT THIS TIME.

1. Overview/Purpose/ Description of Procurement

The DISA RAO is conducting this RFI to explore the business case for a Cloud Based Internet Isolation Capability to support the Agency’s EndPoint Security Solutions Portfolio. The Enterprise Cloud Based Internet Isolation capability would provide defense against a variety of attacks that exploit Department of defense (DoD) networks and compromise end clients. The service would redirect the act of internet browsing from the end user’s desktop into a remote server, external to the Department of Defense Information Network (DoDIN), and deliver as a cloud based service leveraging concurrent (simultaneous) use licenses at ~60% of the total user base (3.1 Million users).

2. Scope of Effort and Technical Characteristics

The prospective solution may utilize multiple geographic locations as necessary which could include the following sites: Warner Robins (GA), Columbus (OH), San Antonio (TX), North Island (CA), Pentagon (DC), Hampton Roads (VA), Yokota (Japan), Ramstein (Germany), Stuttgart (Germany), and Hickam (HI). The solution must be compliant with Federal Information Processing Standards (FIPS) 140-2 cryptographic modules, support DoD public key infrastructure (PKI) authentication either natively or via token from an authentication proxy, be compatible with all DoD approved browsers, and utilize DoD provided Directory service for user profiles. The system may be housed in FedRamp level II certified data center(s). The vendor may provide host and build software as a service (SaaS) and will be responsible for system setup, maintenance of servers, middleware, and operating system (OS) support, and hosting/sustainment.

The Enterprise Cloud Based Internet Isolation capability may consist of the following areas:

a. 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
   a.a.i. isolate all Internet code execution in the cloud
   a.a.ii. isolate each session in the cloud
   a.a.iii. provide the ability to route internet browsing activity of Android and iOS mobile devices (not connected to DoDIN) via the solution
   a.a.iv. support Role-Based Access Control (RBAC) and grant system administrators access to configure as required by the user role
   a.a.v. support data encryption and encrypt the connection between the user endpoint and system host
   a.a.vi. support XSF stripping
   a.a.vii. provide the ability to downgrade video and audio quality for streaming Internet media (configurable Quality of Service (QOS))
   a.a.viii. provide compression to limit bandwidth utilized in delivering rendering of isolated Cloud session back to the client workstation
   a.a.ix. provide non-attribution browsing capability for a restricted set of users
a.a.x. provide the capability to allow a non-attributable user to egress to the internet from geographically diverse locations that are configurable by the user at the start of the session.

b. The solution may securely store and transmit data in a manner that ensures the confidentiality, integrity, availability, and source authenticity of the data.

c. The solution may include a content control software at the host location
   a.c.i. provide for persistent document storage in the cloud
      a.c.i.1. scan persistent documents for malicious code/infection before storing
      a.c.i.2. 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
   a.c.ii. allow blacklisting and whitelisting Uniform Resource Locator (URL)s by category, geolocation, and uncategorized URL blocking
      a.c.ii.1. provide for updating ‘uncategorized’ URL with categorization provided by user within 0-1 hour
      a.c.ii.2. provide the user the ability to update a blacklisted site to a whitelisted site if wrongly categorized within 0-1 hour
   a.c.iii. allow and block file downloads/uploads by file type; allow to open downloaded files within the cloud session

d. The solution may log all web requests and tie the web request to specific users from authentication through session end
   a.d.i. Capture logs from content control software, blacklisting/whitelisting, data about downloaded files, logs based on geolocation and capture geolocation within the logs
   a.d.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

e. The solution may 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(es) if threshold has been exceeded by a configurable amount

f. The system may provide non-repudiation of browser activity
   a.f.i. Shall support all current and legacy web content technologies, support 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)

g. The system may support the ability to configure the user session inactivity timeout

h. The system may support connections to websites utilizing Secure Sockets Layer (SSL) 3.0 and Transport Layer Security (TLS) 1.0-1.3

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

The Government is hopeful that prospective solutions for this need will be able to meet all capability and functional requirements for the effort as outlined above. Prospective solutions for this capability may be conducted on and off government facilities; all responses to this RFI will define possible work location and infrastructure hosting methodology based on scope and statutory requirements.

3. Requested Information

Interested parties are requested to respond to this RFI with a white paper. Submissions cannot exceed 10 pages single spaced, 12-point type with at least one-inch margins on 8 1/2” X 11” page size. The response should not exceed a 5 megabit e-mail limit for all items associated with the RFI response. Responses must specifically describe the contractor’s capability to meet the requirements outlined in this RFI. Oral communications are not permissible. FedBizOpps (FBO) will be the sole repository for all information related to this RFI.

Companies who wish to respond to this RFI should send responses via email no later than 1:00 PM EST on 29 June 2018 to tatyana.a.mchenry.civ@mail.mil

Respondents are requested to focus the whitepaper on the aforementioned capability areas, describing in detail how their expertise and approach is capable of meeting the Government’s requirements; architectural diagrams depicting the solution, and concept of operations describing the end user and administrator experience. Additionally, the respondents shall submit a Rough Order of Magnitude (ROM) for the cost of system setup, maintenance, support, and hosting/sustainment. The ROM does NOT count against the 10 page RFI limited response.

In addition to the RFI vendors are requested to submit a statement of their knowledge and capabilities to perform the following:

a) Describe your experience managing the technical and functional activities associated with operations, maintenance, modifications, engineering, integration, deployment, schedule, and sustainment of Enterprise Cloud Based Internet Isolation solutions.
b) Describe, if applicable, prior experience and working knowledge of Enterprise Cloud Based Internet Isolation solutions.
c) Describe your experience in supporting or implementing system Certification and Accreditation (C&A) efforts through the DoD Risk Management Framework (RMF) by providing examples of successfully fielded system deployments.
d) With consideration to the technical characteristics and requirement’s scope, recommend a method in which the Enterprise Cloud Based Internet Isolation capability would be delivered to the Government. If your firm is capable of delivering the capability solely, provide an estimated
If your firm recommends partnering with other contractors, detail the development and integration efforts needed to provide a single solution.

e) Responses should provide the business’s Data Universal Numbering System (DUNS) number and Commercial and Government Entity (CAGE) code.

The capabilities statement should not exceed 5 pages. Promotional materials are not requested and will not be reviewed.

**INDUSTRY DISCUSSIONS:**
DISA representatives may choose to meet with potential offerors and hold one-on-one discussions. Such discussions would only be intended to obtain further clarification of potential capability to meet the requirements, including any development and certification risks.

**QUESTIONS:**
Questions regarding this announcement shall be submitted in writing by e-mail to amy.ford6.civ@mail.mil. Verbal questions will NOT be accepted. Answers to questions will be posted to FBO. The Government does not guarantee that questions received after 15:00 EST on 26 June 2018 will be answered. The Government will not reimburse companies for any costs associated with the submissions of their responses.

**DISCLAIMER:**
This RFI is not a Request for Proposal (RFP) and is not to be construed as a commitment by the Government to issue a solicitation or ultimately award a contract. Responses will not be considered as proposals nor will any award be made as a result of this synopsis.

All information contained in the RFI is preliminary, as well as subject to modification, and is in no way binding on the Government. FAR clause 52.215-3, “Request for Information or Solicitation for Planning Purposes”, is incorporated by reference in this RFI. The Government does not intend to pay for information received in response to this RFI. Responders to this invitation are solely responsible for all expenses associated with responding to this RFI. This RFI will be the basis for collecting information on capabilities available. This RFI is issued solely for information and planning purposes. Proprietary information and trade secrets, if any, must be clearly marked on all materials. All information received in this RFI that is marked “Proprietary” will be handled accordingly. Please be advised that all submissions become Government property and will not be returned nor will receipt be confirmed. In accordance with FAR 15.201(c), responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract.

**SMALL BUSINESS:**
This RFI is encouraging responses from any qualified and capable source, including Small Businesses, Service Disabled-Veteran Owned Small Businesses, Veteran-Owned Small Businesses, Women-owned Small Businesses, HUBZone Small Businesses, Small Disadvantaged Small Businesses, Historically Black Colleges and Universities/Minority Institutions, Small Business Joint Ventures, Consortiums and Teaming Partners. This RFI is issued to assist the Agency in performing market research to determine whether or not there are two or more qualified and capable Small Businesses to provide the aforementioned service.