REQUEST FOR INFORMATION (RFI)
DISTRIBUTED HYBRID MULTI CLOUD

Prepared by:

DISA COMPUTE OPERATIONS
HC32

07 March 2023

BACKGROUND

The DISA Hosting and Compute Center (HaCC) is transforming the way it is delivering hosting and compute solutions across the Department. This transformational strategy is driving toward solutions that are hybrid, distributed, and multi-cloud. Partnering with industry to achieve these objectives is paramount for success.

The HaCC currently has multiple x86 hosting environments completely isolated and independent of one another. Each environment has different management planes and different processes. To streamline management of assets for both our customers and for our administrators, HaCC aims to develop a management plane that centralizes all current capabilities, with additional improvement capabilities and innovative processes, into a single centralized control plane.

This effort will develop a single environment that rationalizes and encompasses all x86 commodity within the HaCC, merging disparate components into a modernized distributed, hybrid, and multi cloud (DHMC) infrastructure and services offering. This environment will be managed through a single centralized control plane. Commercial cloud assets, on-premises cloud assets, traditional virtualized assets, and dedicated host connected assets will all be managed through a single customizable control plane.

The DHMC solution will be housed in a consolidated stack located within multiple DISA datacenters. This stack should be standardized for eventual, uniform deployment to multiple sites, including OCONUS. This will result in a distributed, hybrid, and multi-cloud environment that is hosted on premises.

The new acquisition will include a modern technology implementation strategy that will achieve a rapid deployment of the new DHMC solution. In addition to a rapid deployment strategy will be a streamlined and modern migration strategy for existing workloads hosted in the Hosting and Compute Center's current x86 environments.

A customizable, unified on-premises control plane will offer a novel, easily managed interface, for both tenants and administrators, to commercial cloud service providers.

The HaCC envisions its new infrastructure having several desired key features and technologies. Integration of these key features and technologies into a customizable, unified on-premises control plane is a Critical Success Indicator:

- Distributed, Hybrid, and Multi-cloud ready
- Hosted on premises
- Unified and customizable control plane for additional internal services
- Multi-Tenancy support with full customer environment segmentation
- Utility based billing and reporting (pay-as-you-go)
- Elasticity and Automated Scalability of physical hardware within the stack
- Role Based Access Control (RBAC) for granular security management of tenant access
- Infrastructure as Code ready for Ansible and Terraform;
- Interoperability support for existing HaCC enterprise level tools
- Automated scalability
- Monitoring and Alerting
- Centralized portal for security posture
- High Availability (HA) implementations for resources
- Integrated file and image level backup solution
- Full disaster recovery and migration solution to allow agnostic migration capabilities
- Tenant Billing portal

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

OVERVIEW/PURPOSE/DESCRIPTION OF PROCUREMENT

To enable DISA's Mission Partners (MP) and HaCC community expedient access to a representative DHMC environment, DISA is leveraging Other Transition Authority (OTA) to quickly develop a functional prototype. It is envisioned that rapid iterations of the initial prototype DHMC environment will be necessary to fully meet all critical success indicators.

The Government intends to pursue an aggressive approach, procuring a minimum viable capability release (MVCR) in less than one year. Following a successful prototype, the Government will continue the improvement, operationalization, and implementation of DHMC capabilities through a follow-on Production OTA.

As a first-of-its-kind DHMC capability with a customizable and unified, highly integrated control plane offering a novel, easily managed interface supporting all defined key features and technologies, the Government intends to prototype evolving iterations of the prototype throughout the execution of this project. Specifically, the Government intends to apply an agile methodology to create, design, develop, and demonstrate the operational utility for a production ready and operationalized DHMC on-premises capability.

MARKET INTELLIGENCE APPROACH

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

- Industry's input and suggestions on refining the key features and technologies required as outlined in this RFI, including foreseen and unforeseen risks and areas that need clarification
- Industry's input and suggestions that would help refine and improve the Government's technical approach
- Industry's feedback on the Government's projected acquisition approach, including the ability to meet the requirements of an OTA under 10 U.S.C. §4022
- Industry's capabilities to meet the acquisition and technical characteristics of this requirement

Respondents to this RFI are invited to participate in a collaborative Program Manager (PM) question and answer (Q&A) session with the Government. The Hosting and Compute Center (HaCC) Director will make opening remarks at this event followed by the PM providing a brief overview of the program and acquisition approach. Following introductions will be a Q&A session where industry can ask clarifying questions surrounding the requirements and future capability. This is intended to provide clarity into the Government's approach and requirement.

PM Q&A details include:

- The event will occur at 0930 EDT on 13 April 2023. The event will be in-person and the venue is to be determined. An amendment to the RFI will be posted outlining the venue details.
- Questions for the Q&A session must be submitted ahead of the event and are due no later than 5 April 2023.
- Companies who are interested in participating in the PM Q&A must RSVP no later than 5 April 2023 to:

Shaun Bright, Agreements Officer, shaun.m.bright.civ@mail.mil
Jeremy Markusic, Agreements Specialist, jeremy.d.markusic.civ@mail.mil
Organization Box, disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil

The Government expects that strong corporate teams, with the ability to apply a broad range of knowledge, skills, and tools, will form the basis of successful offers. To encourage such teaming efforts, the Government intends to allow companies the opportunity to participate in a HaCC DHMC Industry Networking Day. This event will follow the PM Q&A

session on 13 April 2023. Companies will be given the opportunity to provide a 10–30-minute presentation (participation dependent) on their capabilities, for the purposes of partnering with other companies for the acquisition. The presentation materials and contact information provided will be posted to sam.gov along with this RFI for companies to reach out in preparation for the upcoming acquisition.

Companies that are interested in participating in the HaCC DHMC Industry Networking Day must RSVP no later than 5 April 2023 to:

Shaun Bright, Agreements Officer, shaun.m.bright.civ@mail.mil
Jeremy Markusic, Agreements Specialist, jeremy.d.markusic.civ@mail.mil
Organization Box, disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil

TECHNICAL CHARACTERISTICS
See Appendix 2 Statement of Need for the technical characteristics.

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

RESPONSE GUIDELINES
Interested parties are requested to respond to this RFI with a White Paper in accordance with the White Paper Format provided in Appendix 1. Submissions shall not exceed four (4) pages, single spaced, 11-point type with at least one-inch margins on 8 1/2" X 11" page size. Cover pages are not included in the page limit. The response should not exceed a 5MB e-mail limit for all items associated with the RFI response. Responses must specifically describe the contractor's ability to meet the requirements of this effort. Oral communications are not permissible. Companies who wish to respond to this RFI should send responses via email no later than 22 April 2023 to:

Shaun Bright, Agreements Officer, shaun.m.bright.civ@mail.mil
Jeremy Markusic, Agreements Specialist, jeremy.d.markusic.civ@mail.mil
Organization Box, disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil

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 RFI shall be submitted in writing by email to:

Shaun Bright, Agreements Officer, shaun.m.bright.civ@mail.mil
Jeremy Markusic, Agreements Specialist, jeremy.d.markusic.civ@mail.mil
Organization Box, disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil

Verbal questions will NOT be accepted. Answers to questions will be posted to sam.gov and DreamPort.tech. The Government does not guarantee that questions received after 5 APR 2023 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 formal Request for White Papers or a Request for Proposal and is not to be construed as a commitment by the Government to issue a solicitation or ultimately award an agreement. Responses will not be considered as proposals, nor will any award be made as a result of this RFI.

All information contained in the RFI is preliminary as well as subject to modification and is in no way binding on the Government. The Government 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 response to this RFI that is marked "Proprietary" will be handled accordingly. Please be advised that all submissions become Government property and will not be returned. Responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract or agreement.

Non-Government personnel will be used in collecting market intelligence, which includes responses to this RFI. The non-Government advisors may have access to all aspects of the materials received in RFI responses, which includes any documents marked as "Proprietary", as described above. By submitting a response to this RFI, respondents agree with the use of non-Government advisors employed with the following companies:

- 22nd Century Technologies
- Free Alliance, LLC

APPENDIX 1: White Paper Format

Cover Page Information (NOT included in 4-page limit)

Identification	
Company Name	
Company Address	
Point of Contact (Primary)	
Phone Number	
E-mail Address	
Cage Code	
DUNS	
Company Web Page	
Other Classifications (e.g., large business, small business, SDB, HUBZone, 8(a), SDVOSB, WOSB, etc.)	
List Government Wide, DoD, or DISA contracts you are on that are applicable as a Prime or a Subcontractor (Includes partnering on Platform 1)	

Interest

Describe your potential interest in this effort (e.g., prime, subcontract, teaming, joint ventures) and how you would meet the 10 U.S.C. §4022 requirements for qualifying for an OTA.

Corporate Capabilities

Describe your company and any corporate information relevant to meeting the DHMC requirement.

1.0 Technical Recommendations

Provide any recommended technical or development approaches that the Government should consider for this effort, based on the draft Statement of Need (SoN) (Appendix 2). Please provide feedback that helps clarify the SoN and helps ensure the Government meets the DHMC program needs.

2.0 Potential Risks

Provide any potential risks that you foresee from the SoN and the potential prototype. Also provide any recommended risk mitigation approaches that the Government should consider for this effort. This includes any approaches the Government could be unaware of that would support an accelerated schedule to achieve the key features and technologies referenced above.

3.0 Acquisition and Other Recommendations

Provide any recommendations on the Government's projected acquisition approach and any other relevant recommendations to help inform the Government.

4.0 Technical Capabilities

Describe your company's and/or team's ability to meet the SoN. Please include a discussion of potential new development options and the integration of COTS products, as appropriate.

5.0 Rough order of Magnitude (ROM) Cost

Provide a ROM for this effort. Please note that this is not considered a price proposal, nor will this ROM be held against a company that participates in any solicitation that relates to this program. ROMs received as part of this RFI will strictly be used for Government budgetary planning purposes only.

APPENDIX 2: Statement of Need (SoN)

1. Background

Currently DISA's Hosting and Compute Center's x86 virtual environment encompasses several different platforms and offerings. Each of these offerings has a different point of entry for our administrators and customers. The backup and migration processes are different for each of these platforms which results in inconsistencies and difficulties in management. DISA's current on-prem cloud environment lacks several key capabilities that customers looking for cloud capabilities need. Customers are leaving our current environment at an exponentially increased rate due to services offered by other platforms.

As DISA moves forward with the Joint Warfighting Cloud Capability (JWCC) contract, an increasing number of customers will move applications to commercial cloud provider environments. It is expected that the large majority will leverage Amazon Web Services (AWS) and Microsoft Azure. A much smaller subset will leverage Google Cloud Platform (GCP) and Oracle Cloud. Many of these customers will have traditional virtualization, on premise assets, as well as commercial cloud assets simultaneously.

The subject of this SoN will replace the current x86 infrastructure in DISA's Hosting and Compute Center (HaCC) while providing a central management plane between all customer x86 hosted assets. It will standardize management of x86 assets within the HaCC using agnostic supporting services. The subject product will provide a smoother entry into the environment as well as a much smoother transition from traditional hosting into commercial cloud. The product will include various add-on services that will boost its marketability and establish it as a competitive alternative to

2. Statement of Need

DISA's Hosting and Compute Center requires a reimagined x86 hosting solution that incorporates modern cloud technologies and capabilities into a consolidated on-premises stack. This need will be for both Non-classified Internet Protocol Router (NIPR) and Secret Internet Protocol Router (SIPR). The new solution will leverage principles and capabilities from distributed cloud, hybrid cloud, and multi cloud architectures all brought together under a central control plane for asset management. The central control plane will be the single portal through which customers and administrators manage fully segmented and isolated customer environments. The control plane will have direct integration with DISA instances of asset management and compliance tools to provide streamlined automation and drastically reduce the effort involved in asset management and compliance tasks. The solution will also include a customer billing portal from which customers and programmatic personnel can monitor and manage their accounts.

A successful prototype effort for the environment and supporting control plane will accomplish the following. Any characteristic that is not mandatory for successful prototype, but is desired, is annotated as an "objective need".

- The new infrastructure and control plane will provide a single pane of glass for all DISA Hosting and Compute Center's (HaCC) x86 assets. The intent is to provide a single location from which a customer/administrators can manage all their assets. The new environment will have a central control plane for managing:
    - On-premises cloud environment
    - Commercial cloud assets
    - Containers
    - Traditional virtualized assets
    - Dedicated hosts

Distributed, Hybrid, and Multi-cloud ready – interaction from on-premises control plane to public cloud service providers with a specific focus on Amazon Web Services and Microsoft Azure. The solution will have the ability to provision and manage instances in commercial cloud service provider environments. The intent is to enable this solution to provision assets into commercial cloud environments in partnership with Joint Warfighting Cloud Capability (JWCC).

- HaCC's solution will include multi-tenancy support with full customer/account level segmentation. Customers should be able to have all their assets in a single Virtual Datacenter (VDC), Virtual Private Cloud (VPC), or Virtual Cloud Network (VCN). The VDCs or VPCs should be fully segmented from one another and have their own firewall capabilities. Multi-tenancy capabilities should include the following:
    - Single point of entry for each customer to their entire cloud environment
    - Single control plane representation of all customer assets in one place regardless of location or offering
    - Customers are separated from each other and exist in isolated environments
    - Data is kept completely private and encrypted
    - Ability for infrastructure and tenant-controlled encryption keys with Virtualized Traditional Physical Module (vTPM) encryption support
    - Network micro-segmentation capabilities
    - Built-in ability for tenants to analyze network traffic entering or exiting their space
    - Capability to monitor traffic inside the tenant boundary

  Solution must be hosted on-premises in a consolidated standardized stack within DISA datacenters. The stack needs to be standardized and concise making it ideal for replication when scaling to other sites. The solution will be leveraged both CONUS and OCONUS making standardized configuration critical for effortless expansion.

- Elasticity - Ability to attach additional or remove existing physical hardware into the stack enabling integration, decommissioning, or provisioning.

- Solution will be constructed leveraging a Zero-Trust architecture.

- Customizable control plane for additional internal services/modules. The portal for the central control plane needs to be easily customizable facilitating integration with various DISA services. Initially, upon implementation, the control plane will need to include custom portals for Cyber, compliance and DISA's Containers as a Service (CaaS) offering. The solution needs to enable the addition of future portal capabilities such as integration with DISA's Database as a Service offering among others. Additionally, the portal must be customizable to facilitate DISA branding and a "look and feel" that DISA approves of.

- Role-Based Access Controls (RBAC) controls including smart card/CAC/PIV authentication. Multifactor authentication and single sign-on support will be a hardline requirement. Customers and administrator access control permissions should be fully customizable.

- Fully functional DevSecOps automation pipeline in place to handle the various requirements of the integrated solution. Deployments, scaling, and other integrated actions leveraging written DevSecOps pipeline style automation should happen seamlessly.

- Interoperability support for existing enterprise tools critical to our workload. Specifically, this would include ServiceNow and Splunk

- Automated scalability with ties to asset management systems for automated asset tracking alongside scaling. Provisioned assets should have lifecycle options available during the provisioning process allowing customers/admins to assign an end-of-life date to the asset.

- *Objective Need: Alert generated scaling in response to alerts.

- Solution will have extensive integrated monitoring and alerting capabilities such as.
    - Realtime insights
    - Alerting features (email and SMS messaging, alerts that trigger scripts or automation tasks, etc.)
    - Cloud-ready manner of monitoring assets/applications/containers/DBs/etc.
    - Infrastructure level monitoring and automated handling of events

- Centralized portal for security posture. The security portal will be a part of the central control plane and should provide full spectrum security reports itemized by environment. The reporting capability should be accessible by customers for on demand generated reports regarding the posture of their environment.

- Solution will need to meet industry standard redundancy capabilities and include simple high availability implementations for resources.

- Platform will need an integrated backup capability that meets government backup requirements. The backup service will need to be agnostic and function well across all asset types.
  Integrated file and image level backups to support:
    - Independent disks
    - Network file storage
    - Storage attached networks
    - Object storage

- Solution will require a modern strategy that facilitates rapid deployment of the new environment while also facilitating a seamless tech refresh process for future upgrades.

- Full disaster recovery and migration solution to allow agnostic migration capabilities. The disaster recovery and migration capability need to facilitate a seamless migration of x86 assets into the environment. This migration process/capability needs to also allow a quick/easy transition of assets from one hosting type to another within the solution. The disaster recovery and migration solution should:
    - Be capable of disaster recovery to specific snapshot in time
    - Be capable of asset migration from on-prem cloud to commercial cloud and vice versa
    - Include Containerized environment disaster recovery and migration capability
    - Support migration of current x86 assets to new solution with minimal downtime and impact to mission
    - Support the migration of existing virtual machines from formats like OVA and VMDK formatted files

- Billing portal should provide billing management capabilities to the program office as well as environment billing features for the customers. Billing portal should include:
    - Full cost transparency for tenants
    - Reporting functionality
    - At-a-glance dashboards
    - Budgeting tools such as billing threshold alerts
    - Customer ability to place server orders in the portal and have servers provisioned via integrated automation

- Platform will have a seamless integration for HaCC's current Containers as a Service (CaaS) platform. This integration will allow the CaaS platform to migrate into the new x86 environment in an efficient and optimal manner.

- Platform will have full OS patch management resources for all x86 UNIX and Windows operating systems.

- New solution will have an included capability that leverages artificial intelligence and machine learning to traverse system and event logs in order to provide preventative resolutions and drastically reduce outage times by reducing the amount of troubleshooting required. Additionally, it is expected that the platform will have machine learning and artificial intelligence leveraged against cyber data. This will give the product the ability to identify exploited vulnerabilities through learned behaviors based on a constant in-depth analysis of events.

- Platform will include a full high-performance compute (HPC) as a service suite that is ready to host high performance computing workloads as a service provided to DISA customers. The HPC service will have its own portal within the management plane. The HPC service will have billing monitored, tracked, and reported on by the billing portal.