Department of Defense Healthcare Management System Modernization (DHSM) Program

Request for Information (RFI) for Hosting

DHSM Program Management Office
DoD Healthcare Management Systems (DHMS) Program Executive Office
1. INTRODUCTION
The Department of Defense (DoD) Healthcare Management System Modernization (DHMSM) Program is a tailored Major Automated Information System (MAIS) program on contract to field a configurable and scalable modernized Electronic Health Record (EHR) System. DHMSM will replace DoD legacy healthcare systems including, but not limited to, Armed Forces Health Longitudinal Technology Application (AHLTA), Composite Health Care System (CHCS) (inpatient), and most components of the Joint Operational Medicine Information System (JOMIS) program, with an Off-The-Shelf (OTS) EHR System. DHMSM will address the current state of the Military Health System (MHS), where multiple healthcare legacy systems and data stores, developed over decades, are in need of modernization to ensure and enable sustainability, flexibility, and interoperability, for improved continuity of care.

The DHMSM program awarded a contract on July 29, 2015 to deliver an integrated inpatient / outpatient Best of Suite (BoS) EHR solution, augmented by Best of Breed (BoB) product(s). BoS refers to an integrated inpatient and outpatient EHR System with software components that to the maximum extent practical allow for integrated, maintained, and deployed with a design architecture that allows for access to and sharing of common data, common user interfaces, common workflows, and common business rules. Furthermore, a BoS will support end-to-end related healthcare and business operations. BoB is defined as a solution or module not part of the BoS, which would require engineering and integration efforts in order to be integrated with the BoS. When implemented, the EHR System will provide access to authoritative sources of clinical data to enable improved population health, patient safety, and quality of care. The solution will support an enhanced patient care experience and serve as a tool to maximize medical readiness for our military.

The modernized EHR System will unify and increase accessibility of integrated, evidenced-based healthcare delivery and decision-making. The DHMSM program is collaborating with the DoD/Department of Veterans Affairs (VA) Interagency Program Office (IPO) and the Defense Medical Information Exchange (DMIX) program to ensure compatibility and interoperability with the standardized healthcare data framework and exchange standards, promulgated by the Office of the National Coordinator for Health Information Technology (ONC) to enable the exchange of health data. DHMSM supports the availability of longitudinal health records for over 9.6 million DoD beneficiaries and over 153,000 MHS personnel globally, and to the full range of military operations to DoD practitioners wherever and whenever needed. The application of standardized workflows, integrated healthcare delivery, and data standards will enable improved electronic exchange of health and patient data between the DoD and its external partners, including the VA and other Federal and private sector healthcare providers.

2. DHMSM AND DEFENSE HEALTH AGENCY (DHA) HEALTH INFORMATION TECHNOLOGY INFRASTRUCTURE (HIT)
The DHMSM solution leverages the existing DoD IT Networks (DODIN) as well as the DHA HIT infrastructure enclave for support to the EHR application. The Medical Community of Interest (MED COI) provides for this HIT backbone which supports the legacy EHR capability as well as the new DHMSM EHR.

In addition to this infrastructure, DHMSM requires a hosting solution for the new EHR and data supporting the EHR solution. The DHMSM EHR contractor will use a centralized data and services architecture, which will rely on one primary data center as well as an alternate back up data center to
provide continuity of care to the DHMSM EHR users. The performance standards at the primary and backup data centers must be comparable to or exceed those at a DISA data center. This RFI is part of market research activities being performed by the DHMSM program office to ascertain which hosting options are available and may meet its EHR hosting requirement.

Within this hosting requirement, the DHMSM EHR contractor must retain direct operational configuration and control of the application and data including managing the hardware from the hypervisor up as well as logical networking. Therefore RFI responses should only be from sources who delegate operational configuration and control of the environment. The hosting solution must be ready to support a contract award in the January 2016 time period and must be ready to host the DHMSM EHR application by 1 February 2016 to the DoD IOC delivery timeline. The hosting facility must have a FEDRAMP level 4 certification for handling sensitive/Personal Health Information (PHI) information. Given the critical relationship between the hosting contractor and the DHMSM EHR contractor, only hosting contractors prepared to execute a Memorandum of Agreement (MOA), Associate Contractor Agreement (ACA), or other similar agreement with the DHMSM EHR contractor should respond to this RFI.

3. QUESTIONS

3.1. SECURITY

a) Is your hosting capability connected to the DoD IT Network (DODIN) network? If not, are you in process to obtain such a connection? If so, when do you expect to receive it?

b) Is there a US Federal Government Access Point in place at your hosting facility/facilities? If not, are you in the process of implementing one? If one is in process, when is it expected to be in place?

c) Is your hosting capability exclusive for the US Federal Government (physical or logical)? If not, what are the restrictions on the use of your infrastructure?

d) Is your data center and computing services managed and operated by U.S. citizen staff and have the proper clearances for handling sensitive/Personal Health Information (PHI)?


f) Have you previously hosted a system with a DoD Information Assurance Certification and Accreditation Process (DIACAP) or Risk Management Framework package (DoDI 8500.01 and DoDI 8510.01) ATO? If so, please describe.

g) What type of encryption does your hosting solution allow or enable for data at rest?

h) Would your hosting facility allow United States CYBERCOMAND the capability to monitor the security status of your hosting capability? If so, describe how you would allow this to occur.

i) Will you be willing to put a Government owned and managed MED COI CAP in your hosting facility? If so, describe any conditions for allowing this to occur.

3.2. PHYSICAL

a) In which states and countries are your data centers (DCs) located (USA jurisdiction under US laws and regulations)?

b) What kind of physical security measures are in place?

c) What are the nationalities of the people who have access to your data centers (e.g., only US citizens)?
d) Do you have redundant data center locations at a minimum 150 miles from the DISN Point of Presence (PoP)?
e) What speed is your internal network (e.g., 40 Gbps)?

3.3. CAPACITY

a) Approximately how much capacity can your data center provide as of January 1, 2016? You should supply numbers for each of the data centers that will be involved.
b) Do you offer on demand scalability (elasticity)? If the answer is yes, is there a limit on this scalability (how many virtual servers) for our use as of January 1, 2016? [Assume a medium sized server with 2 virtual CPUs and 4 GB RAM]
c) Do you offer virtual server choices? (e.g., tiny, small, medium, large, GPU focused) If so, describe what varieties you offer. What are their prices?
d) Do you offer reserved physical servers (exclusive use of particular servers for our applications)? If so, what is the cost?
e) What kinds (e.g., SSD, spinning media) of storage do you offer and in what quantities? The answer may be approximate. Do you offer reserved instances? If so, what is the cost?

3.4. COST/PRICING

a) What is your hosting data center pricing structure?

3.5. MANAGED SERVICES

a) Do you offer active monitoring and would it be made available to DoD for an integrated view (e.g., of VMs and storage)? If so, what do you monitor that the application owner can see (e.g., consumed host memory, consumed host storage, uptime)? If so, how often is it updated (e.g., hourly, monthly)? If so, can the DoD access this and to what level (e.g., user level access, automated data feed, etc)?
b) Do you have a standard Service Level Agreement (SLA)? If so, please attach it or give the link to an URL.
c) Do you offer automated monitoring of your SLA?
d) Do you offer application SLA monitoring?
e) Do you offer metering? If so, what is your minimum unit of charge time (e.g., hour, month, year)?

3.6. SCALABILITY

For the next few questions, assume that the application in question was written to scale horizontally (e.g., stateless, etc.).
a) Do you offer the ability to scale the application out (i.e., add new instances and load balance across them)?
b) Do you offer the ability to scale down the application (i.e., remove instances and remove them from the load balancer)?
c) Can you scale the application out automatically, based on a trigger that the application owner sets (e.g., when CPU or RAM reaches a threshold)? If so, what triggers do you support (e.g., CPU, RAM)?
d) Can you scale down (remove instances of) the application automatically, based on a trigger?
e) Can you scale an application out, based on a timeframe (e.g., every Friday from 4:00 to 5:00 PM EST)?
f) Can you scale down an application, based on a timeframe?
g) Do you offer block storage (direct attached storage used by running VMs)?
h) Do you offer file storage, including the ability to create, update, read, and delete files?
i) What is the MTBF for this service?
j) When a file is saved, how many copies of the data are written, and where (e.g., in another drive, another server, another cluster, another data center)?
k) Describe any encryption capabilities associated with the file storage service.
l) Do you offer a notification service that can notify an administrator when an event occurs (e.g., a virtual machine crashes, or a monetary threshold is reached)? If so, what forms of notification does it offer (e.g., email, SMS, etc)?
m) What kinds of triggers does it offer (e.g., monetary threshold, number of VMs)?
n) Do you allow remote administration and management of the OSs and/or HYPERVERSOR? What OSs or HYPERVERSORs do you support?

3.7. CONTINUITY
Disaster Recovery encompasses the policies and procedures to prepare for recovery of technology infrastructure and business operations critical to an organization after a natural or human-induced disaster to partially or completely restore services and critical functions within a predetermined time after a disaster or extended disruption.

a) What are your Continuity of Operations and Disaster Recovery (COOP/DR) capabilities?
b) What is your current plan for network and hosting diversity?
c) Where are the COOP/DR sites for your hosting capability?
d) Does your COOP/DR capability require synchronous replication, so we would expect a COOP data center to be close to allow that replication to occur?

3.8. ENVIRONMENTS

a) Upon award, how long would it take to provide this hosting capability?
b) Do you offer a Virtual Private Cloud (VPC) that would encapsulate all our workloads? If so, do you offer a dedicated connection to the VPC from another Data Center?
c) What is your current Data Center Infrastructure Efficiency (DCiE)? This metric is the ratio of the IT equipment energy to the total data center energy use. The total data center energy use is the sum of the electrical energy for IT, HVAC system, power distribution, lighting, and any other form of energy use, like steam or chilled water. All the energy data values in the ratio are converted to common units.
d) Does your Company make use of the ITIL standards: makes use of ITIL service strategy and industry-best standards, incident management, problem resolution, service provisioning, etc.? If so, what Service Model do you provide: Platinum, Gold, Bronze, etc.?

3.9. SPECIFIC SERVICES

a) Do your services include a logging service? If so, would that be available for the government’s use? What technology do you use for logging (e.g., Splunk, Sumo)?
b) Do you offer a patching service, a service that could patch VMs? If so, can it patch a running VM? Can it patch a stored VM file (e.g., VMDK file)?
c) Do you offer a PaaS? If so, which PaaS stack does it use (e.g., OpenShift, CloudForms)? What application server does it support (e.g., JBoss, Spring)?

d) Do you support Docker? If not, do you support a similar container?

4. PERFORMANCE

The hosting capability must support as a System of Systems (SoS) the following technical performance measures that the DHMSM EHR overall solution must meet. The allocated performance baseline will be assigned to the hosting solution, but it will be a higher level of performance that these SoS performance measures contained in Table 4-1 below.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System MTBF (Min)</td>
<td>5,000 hours</td>
<td>The system shall meet minimal Mean Time Between Failure (MTBF) requirement. MTBF failures are considered to be those out of design conditions which place the system out of service and into a state for repair. Calculated by summing the operational periods divided by the number of observed failures during which the system was unable to support critical operations. (MTBF = Start of Down Time - Start of Up Time)/Number of Failures)</td>
</tr>
<tr>
<td>System MTBCF (Min)</td>
<td>9,000 hours</td>
<td>The system shall meet minimal Mean Time Between Critical Failure (MTBCF) requirement. MTBCF calculation failures are considered to be those out of design conditions that place the system out of service and into a state for repair. Applies to system-wide services and services supporting critical capabilities at every level such as Emergency Rooms, Intensive care units and like activities (MTBCF = Start of Down Time - Start of Up Time)/Number of Critical Failures)</td>
</tr>
<tr>
<td>Scheduled Shutdowns (Max)</td>
<td>5 / year</td>
<td>The system shall not exceed the number of scheduled system shutdowns per year threshold</td>
</tr>
<tr>
<td>Software Component MTTR (Max)</td>
<td>6 hours</td>
<td>The system shall meet component software Mean Time to Repair (MTTR) threshold. Total volume of incidents reported automatically by monitoring systems and calculated as Total Incident Time Open + 6 hours</td>
</tr>
<tr>
<td>Hardware Component MTTR (Max)</td>
<td>12 hours</td>
<td>The system shall meet component software Mean Time to Repair (MTTR) threshold. Total volume of incidents reported automatically by monitoring systems and calculated as Total Incident Time Open + 6 hours</td>
</tr>
<tr>
<td>System MTTRS (Max)</td>
<td>1 min</td>
<td>The system shall meet Mean Time to Repair System (MTTRS) threshold needed to switch to a redundant backup unit</td>
</tr>
</tbody>
</table>
Metric | Time | Description
--- | --- | ---
Operational Availability ($A_0$) | 99.90% | The system shall meet System Operational Availability ($A_0$) threshold to assess the total time the system is capable of being used to perform clinical functions during a given interval using the Mean Time Between Failure (MTBF) divided by the sum of the MTBF, Mean Time to Restore (MTTR), and Mean Logistics Delay Time (MLDT) \[A_0 = \frac{MTBF}{MTBF + MTTR + MLDT}\]

Critical Operational Availability (C-$A_0$) | 99.99% | The system shall meet critical clinical system and application availability (e.g., Emergency Rooms, Intensive care units and like activities) to support critical care provided at individual medical units wherever they are located (Garrison and Theater). Mean Time Between Critical Failure (MTBCF) divided by the sum of the MTBCF, Mean Time to Restore (MTTR), and Mean Logistics Delay Time (MLDT) \[A_0 = \frac{MTBCF}{MTBCF + MTTR + MLDT}\]

5. INSTRUCTIONS FOR SUBMISSION

RFI respondents are encouraged to provide responses and comments to the questions above. Responses and comments may be utilized in the development of additions or modification to future draft RFPs. Responses to the RFI must be submitted by 29 September 2015 at 12:00 PM Eastern Time. All submissions should be uploaded to the SPAWAR e-commerce central website: https://ecommerce.spawar.navy.mil


No verbal or e-mailed responses will be accepted. Proprietary information may be submitted; however, RFI respondents are responsible for adequately marking proprietary, restricted or competition sensitive information contained in their response. All submissions will be protected from disclosure outside of the DHMSM Program Office.

In addition, RFI respondents should be aware that the DHMSM Program Office may utilize contractor support personnel from the below listed companies (under existing contracts) to review responses and information submitted. These companies and individual employees are bound contractually by Organizational Conflict of Interest and disclosure clauses with respect to proprietary information, and they will take all reasonable action necessary to preclude unauthorized use or disclosure of an RFI respondent’s proprietary data. RFI responses MUST clearly state whether permission is granted allowing the program office support contractors identified below access to any proprietary information.

- The MITRE Corporation
- Booz Allen Hamilton, Inc.
- Technatomy Corporation
- Deloitte Consulting
- SeKON Corporation
6. DISCLAIMER

The government does not intend to award a contract on the basis of this RFI or otherwise pay for information received in response to the RFI. This RFI is issued for information and planning purposes only and does not constitute a solicitation. All information received in response to the RFI that is marked Proprietary will be handled accordingly. The Government shall not be liable for or suffer any consequential damages for any proprietary information not properly identified. Proprietary information will be safeguarded in accordance with the applicable Government regulations. Responses to the RFI will not be returned nor will the Government confirm receipt of the RFI response. Whatever information is provided in response to this RFI will be used to access tradeoffs and alternatives available for determining how to proceed in the acquisition process. In accordance with FAR 15.201(e), responses to this RFI are not offers and cannot be accepted by the Government to form a binding contract.