**CUSTOMER REQUIREMENTS STATEMENT**

***Cloud Hosting***

***For***

***Product Lead (PL) Acquisition Management Support Solutions (AMS2)***

**15 August 2017**

**1.0 GENERAL.** Cloud Hosting for Product Lead (PL) AMS2 under the General Fund Enterprise Business Systems (GFEBS) portfolio. AMS2 requires Infrastructure as a Service (IaaS) cloud hosting at impact level 4 for their infrastructure migration to the cloud. Additional applications will transition into the cloud as data centers continue to close.

**2.0 BACKGROUND.** AMS2 is a Materiel Developer charged with providing the Army Acquisition community with a rich set of enterprise capabilities and services that leverage authoritative data from across the Acquisition Domain. The vision for AMS2 is to be the premier source of information technology solutions that enable information dominance at all levels of the Army acquisition enterprise. The program’s mission is to deliver innovative and adaptive solutions that streamline the collection and analysis of data to support the business of doing acquisition. This requires the PL to design, develop, and deploy services according to the Combat Developer’s requirements in a rapid fashion; maximizing re-use where appropriate, and reducing administrative burdens to the greatest extent.

**3.0 SCOPE.** The purpose of this procurement is to obtain commercial cloud hosting within a Commercial Off-Premise Infrastructure as a Service (IaaS) Impact Level 4 cloud environment (Impact levels are defined in the DoD Cloud Security Requirements Guide (SRG)). The Contractor shall deliver an Impact Level 4 IaaS cloud offering as defined in the SRG. The contractor shall provide an IaaS capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run software, which includes operating systems and applications. The Contractor shall also provide cloud capabilities to centrally manage, track, and report cost and performance data for applications hosted within the cloud. The Government will retain control over operating systems, storage, and deployed applications; and limited control of select networking components (e.g., host firewalls). The IaaS cloud service offering must have a signed DoD Provisional Authorization (DoD PA) for IaaS Impact Level 4 at award.

The Government is responsible for the operation and maintenance of the applications and operating systems, and application certification and accreditation. All changes to the Government’s cloud infrastructure for their applications will be processed by the Contractor as directed by the Government.

**3.1 Objectives.** Commercial Cloud Hosting shall be provided in accordance with Government policies listed in the Applicable Documents, Section 4.

The objectives of this task are as follows:

1. To obtain a secure cloud hosting that enables scaling of infrastructure and application resources to meet evolving application and user demand.
2. To have daily visibility into resource utilization.
3. To provide capabilities that meet performance thresholds and to set up and receive notifications when violations occur.

**4.0 APPLICABLE DOCUMENTS.** The Contractor shall adhere to the following documentation, or any revisions/updates thereof where approved for implementation and all applicable regulations, publications, manuals, and local policies and procedures.

* WARNORDs, OPORDs, TASKORDs, CTOs, etc.
* Defense Information Systems Agency, DoD Cloud Services Support website. <http://.disa.mil/computing/cloud-services/cloud-support>
* Defense Information Systems Agency, the Security Technical Implementation Guide (STIG) Home Page; <http://iase.disa.mil>
* Department of Defense (DoD) Concept of Operations (CONOPS) for Cloud Computer Network Defense (CND) DRAFT version 1 dated 21 September 2015
* DoD Cloud Connection Process Guide, Version 2.0 March 2017; <http://www.disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf>
* International Traffic and Arms Regulation (ITAR)
* 36 CFR 1194 Implementing section 508 of the Rehabilitation Act of 1973; Clinger-Cohen Act of 1996 also known as the “Information Technology Management Reform Act of 1996”
* 5 U.S.C.552a Privacy Act of 1974
* CJCSI 6510.01F Information Assurance and Support to Computer Network, 9 February 2011
* CJCSI 6510.0D Information Assurance (IA) and Computer Network Defense (CND), 15 October 2010
* CJCSM 6510-01B Cyber Incident Handling Program, 10 July 2012
* CYBERCOM CTO 10-084 USB Flash Media/Thumb Drive Devices are Prohibited in DoD, 2010
* DoD 5205.02-M DoD Manual Operations Security Manual, 03 November 2008
* DoD 5220.22-M DoD Manual- National Industrial Security Program Operating Manual (NISPOM), 28 February 2006
* DoD 8570.01-M Information Assurance Training, Certification, and Workforce Program Manual, 24 January 2012
* [DoD Cloud Computing SRG](http://iase.disa.mil/cloud_security/Lists/Cloud%20SRG) DoD Cloud Computing Security Requirements Guide Version 1, Release 3 (SRG), 06 March 2017
* DoD Directive (DoDD) 5000.01 The Defense Acquisition System, 12 May 2003
* DoD Directive (DoDD) 8000.01 Global Information Grid Overarching Policy Certified, 10 February 2009
* DoD Instruction 5000.02 Operation of the Defense Acquisition System, 07 January 2015
* DoD Instruction 5015.02 Records Management Directive, 24 February 2015
* DoD Instruction 5200.02 DoD Personnel Security Program, Change 1, September 2014
* DoD Manual (DoDM) 5200.01 Vol 3 DoDM 5200.01, Information Security Program: Protection of Classified Information, Volume 3, 19 March 2013
* DoD Manual 5220.22-M DoD National Industrial Security Program Operating Manual, 28 February 2006; Incorporating change 1, 28 March 2013
* DoD 8530.01 Computer Network Defense (CND) Service Provider Certification and Accreditation Process, 07 March, 2016
* DoDD 5205.02E DoD Directive Operations Security (OPSEC) Program, 20 June 2012
* DoD 5210.50 Unauthorized Disclosure of Classified Information to the Public, 27 October 2014
* DoDD 5220.22 DoD Directive- National Industrial Security Program, 27 September 2004
* DoDD 5230.29 Security and Policy Review of DoD Information for Public Release, 13 August 2014
* DoDD 8140.01 DoD Directive 8140.01, Cyberspace Workforce Management, 11 August 2015
* DoDI 5200.01 DoD Information Security Program and Protection of Sensitive Compartmented Information, 13 June 2011
* DoDI 5230.24 Department of Defense Instruction Distribution Statements on Technical Documents, 23 August 2012
* DoDI 8500.01 Cybersecurity, 13 March 2014
* DoDI 8500.02 Information Assurance Implementation
* DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014
* DoDI 8520.03 Department of Defense Instruction Identity Authentication for Information Systems, 13 May 2011
* DoDI 8520.2 Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
* DoDI 8551.01 Ports, Protocols, and Services Management (PPSM), 28 May 2014
* DoDI 8570 Information Assurance
* DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems, 06 June 2012
* DoDM 5200.01, Vol. 3 Department of Defense Manual Information Security Program: Protection of Classified Information, 24 February 2012, Incorporating Change 2, 19 March 2013
* DoDM 5200.2-R DoD Manual 5200.2-R: Personnel Security Program, February 1996
* DTM-08-003 Next Generation Common Access Card (CAC) Implementation Guidance, 01 December 2008
* Executive Order 13526 Next Generation Common Access Card (CAC) Implementation Guidance, 01 December 2008
* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems, February 2004
* FIPS 200 Minimum Security Requirements for Federal Information and Information Systems, March 2006
* FIPS PUB 140-2 Security Requirements for Cryptographic Modules, 03 December 2002
* FIPS PUB 201-1 Federal Information Processing Standards Publication Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
* FISMA Act of 2002 Federal Information Management Act (FISMA) of 2002
* NIST SP 800-145 The NIST Definition of Cloud Computing, September 2011
* NIST SP 800-53 The Recommended Security Controls for Federal Information Systems and Organizations, Revision 4, April 2013
* Army Regulation (AR) 25-2 Information Assurance
* Army Regulation (AR) 530-1 Operations Security
* Army Regulation (AR) 380-5 Army Information Security Program

**5.0 PERFORMANCE REQUIREMENTS**. The Contractor shall provide an IaaS commercial cloud hosting solution that aligns to the SRG working definitions.

5.1. Online Tool Requirements. The Contractor shall provide online administration and monitoring tools to the Government for context filtered reporting and Government virtual infrastructure metrics for analysis. The Government shall approve role based accounts for access to the tools.

5.2 The Contractor shall provide graphical web-based and command line Cloud Management Functionality (CMF) that is accessible via Army imaged end user workstations for the Government’s management of the infrastructure. Functionality shall be controlled via configurable role-based user accounts. These accounts shall be highly-customizable and at a minimum include the following access rights:

1. Restrict access to each component of the console (e.g., restrict provision resources or view reports)
2. Define access rights for accessible components (e.g., scope of access, read-only versus read-write access)
3. Administrator roles with the ability to create, modify, delete, and configure user accounts, profiles and permissions

5.3 Utilization and Manage Alerts and Reporting. The Contractor shall provide the capability for the Government to continuously monitor utilization and configure real time alarms and alerts. This capability shall include, but is not limited to the following:

1. General health and availability
2. Resource utilization and other events such as failure of service, degraded service, etc. via service dashboard and other electronic means
3. Utilization Measurements
4. Historical utilization for all resources (CPU, memory, storage)

e) Customizable reports to group resources by entity, application, and server

|  |
| --- |
| 5.4 Service Incident Response. The Contractor shall ensure that any incidents regarding remote access to cloud infrastructure or tools are resolved within the performance threshold time. |

5.5 Financial Management Reporting. The Contractor shall provide clear access and visibility to an automated Financial Management Reporting capability for all resources consumed via role-based accounts. The capability shall include:

1. Financial consumption per resource
2. Price calculator or simulator that shall facilitate Government forecasting and financial planning.

5.6 Price and Billing Requirements. The Contractor shall meet the following pricing and billing requirements.

1. The Contractor shall allow the Government to download or receive electronic detailed billing reports that list costs on a resource-by-resource basis. The detailed bill shall itemize each individual billable item to allow Government the ability to perform analytics on which cloud assets are contributing to cloud costs.
2. The Contractor shall provide, upon Government request, a running total of accrued cost for a Government specified timeframe, accurate to within one day of usage. This shall ensure the Government’s ability to scale and meet financial targets.
3. Price breakdown per unit consumed per day/month/year

5.7 Provisioning Resources and Virtual Machines (VM) with a Burstable Performance Billing Model.

5.7.1 The Contractor shall provide demand based provisioning of VMs.

5.7.2 The Contractor shall provide the Government the ability to express server configuration as code or templated configuration allowing for the predictable and repeatable deployment of VM’s.

5.7.3 The Contractor shall provide utilization metric load balancing with the capability to scale up and down by creating and starting or stopping new instances of VM images. These VMs shall be created or terminated as needed in response to changes in user traffic, system resource levels, and application usage.

5.7.4 The Contractor shall provide a variety of storage options to meet the changing and growing needs of PM AcqBusiness.

5.7.5 The Contractor shall provide long term highly durable storage.

5.7.6 The Contractor shall provide a block storage with encryption.

5.8 Auditing, Monitoring, and Logging Capabilities.

5.8.1 The Contractor shall provide a robust logging solution that allows for both machine level logging and higher-level log aggregation.

5.8.2 The Contractor shall provide a method for the automated archival of older logs and the capability to delete logs on a given retirement schedule.

5.8.3 The Contractor is required to provide real-time visibility and 24x7x365 monitoring to include server utilization, uptime, latency, usage, and outages.

5.8.4 The Contractor shall provide the capability for sending notifications to users via email and other means such as SMS or mobile applications. This capability shall allow customization of notification triggers.

5.9 Security.

5.9.1 Information Assurance (IA) Requirements. The Contractor shall comply with all requirements and guidelines provided in the Department of Defense Cloud Computing Security Requirements Guide (DoD CCSRG). The Contractor shall make all changes necessary to comply with future changes in the DoD CCSRG.

5.9.2 The Contractor shall provide the administration, access, and management controls necessary to support the Government.

5.9.3 The Government shall have access to the management console and the ability to administer all of its functions.

5.9.4 Prior to any Government system updates or patches the Government shall be notified and approve the system updates and patches.

5.9.5 The Government shall have complete control of VMs created and shall have root access to each VM to enable any required software or configuration changes.

5.9.6 The Contractor shall allow the Government to implement security groups and network control lists to enable inbound and outbound filtering at the instance and subnet levels as well as assignment of static IP addresses to VMs.

5.9.7 The Contractor shall allow for the creation of a private network within which the infrastructure can operate that is completely un-routable to entities outside the infrastructure. The Government shall have complete control over the management of this virtual network, to include but not limited to, the creation of subnets, the configuration of routing tables, and the inclusion or exclusion of network gateways.

5.9.8 Continuity of Operations (COOP)/Disaster Recovery (DR). The CSP shall provide a COOP/DR capability IAW DoD SRG section 5.10.3.3.

5.9.9 Cyber Security Requirements. Cyber security incidents must be reported within one hour of verified incident to United States Computer Emergency Readiness Team (US-CERT) and executed in accordance with approved Incident Response Plan delivered in the Assessment and Accreditation package. The contractor shall also notify the Government Cybersecurity Lead and the PCO. For cyber security incidents please refer to the SRG, CJCSM\_6510-01B, Cyber Incident Handling Program, NIST SP 800-61, and Computer Incident Handling Guide. For a complete listing of applicable documents please refer to Section 2.

5.9.9.1 The Government Cybersecurity Lead will provide information of DoD notifications (CTO, OPORDS, WARORDs, etc.) to the Contractor to meet compliancy for the Government Granted ATO.

5.9.9.2 The Contractor shall report status to the Government Cybersecurity Lead on the required notifications for compliancy.

5.9.9.3 Prior to assigning cost/invoicing against this contract, the Contractor shall comply with security guidance in accordance with the Department of Defense Contract Security Classification Specification, DD Form 254.

5.9.9.4 The Contractor shall track Contractor Customer Virtual Environment (CVE) administrator accounts' compliance with DoD Cybersecurity Workforce (CSWF) certification requirements, per DoDI 8500.1.

5.9.9.5 The Contractor shall be compliant with DoDD 8140.01.

5.9.9.6 The Contractor shall ensure that Contractor personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoDD 8140.01, Cyberspace Workforce Management. The Contractor shall meet the applicable information assurance certification requirements.

5.10 Government Furnished Equipment and Information (GFE/GFI). The Government does not anticipate Government Furnished Equipment shall be required under this contract. Government Furnished Information is provided at Appendix/Exhibits to this CRS. Any additional /future GFI shall be provided to the Contractor when required by the Government or requested by the Contractor.

5.11 Place of Performance. The primary place of performance under this contract will be at Contractor Facilities IAW the requirements in the Cloud Computing Security Requirements Guide (CC SRG).

5.12 Period of Performance. The period of performance shall be for a twelve (12) month base period with four (4) twelve (12) month option periods.

5.13 Travel. The Government does not anticipate any required travel under this contract.

**TECHNICAL EXHIBIT A**

AMS2 will be migrating its capabilities to the cloud. The initial baseline requires the resources specified below.

SUMMARY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VCPU | RAM (GB) | STORAGE (TB) | WINDOWS (Virtual) | LINUX  (Virtual) |
| 250 | 950 | 10 | 50 | 35 |

\*Table above includes storage necessary for backups, however the percentage of the total storage necessary for backups is application specific. Table does not include disaster recovery compute capacity.

BREAKDOWN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Quantity** | **OS** | **CPU** | **Memory (GB)** | **Attached Storage (GB)** |
| 40 | Windows | 2 | 4 | 100 |
| 10 | Windows | 4 | 15 | 300 |
| 5 | RHEL | 8 | 15 | 200 |
| 15 | RHEL | 2 | 8 | 150 |
| 15 | RHEL | 4 | 15 | 100 |

NETWORK

|  |  |
| --- | --- |
| **Elastic IPs** | **Network Data Transfer Out of Cloud** |
| 50 | 1 TB/Monthly |

**TECHNICAL EXHIBIT B**

**As of June 2017**

The following software and operating systems are utilized in the AMS2 environments:

Red Hat Enterprise Linux

Windows 2012

Oracle

Microsoft SQL Server

LifeRay

JBoss

Apache

.NET IIS

Cold Fusion 10.x

Word press