REQUEST FOR PROPOSAL (RFP) FOR SETTING UP OF DATA CENTER & DISASTER RECOVERY CENTER BASED ON INFRASTRUCTURE AS A SERVICE (IaaS) PLATFORM FOR ERP SAP S/4 HANA SYSTEM FOR THE PERIOD OF SIX YEARS AND EXTENDABLE UPTO THREE YEARS

CIN No. U29190PN2021GOI203505

पंजीकृत पता : गोला बारुद निर्ाण, खड़की, पुणे, महाराष्ट्र – 411 003.

निगनर्त कार्ालर् पता: दूसरी रंनजल, त्र्ानत रूनिट्री, िगर रोड, रेरवडा, पुणे - 411 006

Regd. Address: Ammunition Factory, Khadki, Pune, Maharashtra – 411 003.

Corporate Office Address: 2nd Floor, Nyati Unitree, Nagar Road, Yerwada, Pune – 411 006

दूरभाष सं / PHONE No. 020-67080400,

Email: mil-pune@munitionsindia.in

Web Address: https://www.munitionsindia.in

Table of Contents

NOTICE INVITING REQUEST FOR PROPOSAL (RFP)

1. On behalf of the Chairman and Managing Director, Munitions India Limited (MIL) hereby invites tender for

2. "REQUEST FOR PROPOSAL (RFP) FOR SETTING UP OF DATA CENTER & DISASTER RECOVERY CENTER BASED ON INFRASTRUCTURE AS A SERVICE (IaaS) PLATFORM FOR SAP S/4 HANA SYSTEM FOR THE PERIOD OF SIX YEARS AND EXTENDABLE UPTO THREE YEARS", - as per following details:

Office of Issue:	Munitions India Limited A 100 % Government Owned Enterprise Ministry of Defense 2nd Floor Nyati Unitree, Nagar Road, Yerwada, Pune – 411006. Contact: 020-67080400 mil-pune@munitionsindia.in
Tender (cum RFP) Enquiry No.:	Mod/ERP-PROJ/A/01/2024-25/ADVT/BF

3. This **RFP** is issued without any financial commitment. The Buyer reserves the right to amend or modify any part of the RFP at any stage. Such amendments/modifications to the RFP, if any, shall be duly notified similarly as the RFP. The Buyer reserves the right to withdraw the RFP at any stage, shall it so become necessary.

4. **Validity of Offer:**

Bids shall necessarily remain valid for 180 days from the specified last date for Bid submission. The period of validity may be extended if required. In exceptional circumstances, at its discretion, MIL may solicit the bidder's consent for an extension of the validity period. The request and the responses thereto shall be made in writing or email.

5. **Effective Date of the Contract:**

Unless the consequent Contract specifically defines a different effective date-of-the-contract, the effective date-of-the-contract shall be the date on which the Parties to the Contract have affixed their respective signatures on the Contract or the date of Purchase Order. The Contract shall come into effect on the effective date and remain valid until the completion of the obligations of the Parties under the Contract. The deliveries, supplies and performance of the services under the Contract shall commence from the effective date-of-the-contract.

6. **The RFP is divided into 6 Section as follows:**

(a) **Section I:**

Contains General Information and Instructions for the Bidder about the RFP.

(b) **Section II:**

Contains Essential details of the items/services required, such as the Schedule of Requirements, Delivery Period, which will form part of the consequent Contract with the Bidder.

(c) **Section III:**

Contains the detailed Scope of Work.

(d) **Section IV:**

Contains Standard Conditions of RFP, which will form part of the consequent Contract with the Bidder.

(e) **Section V:**

Contains Special Conditions applicable to this RFP and which will also form part of the consequent contract with the Bidder.

(f) **Section VI – Annexures & Formats:**

7. The usage of the term **'Proposal'** in the RFP, unless repugnant to the context, refers to the Proposal (including the documents, financial instruments, required to be submitted).

8. The usage of the term **'Bidder' or 'ISP'** in the RFP, unless repugnant to the context, refers to M/s RailTel Corporation of India, ISP (Infrastructure Service Provider) in the RFP.

9. The usage of the term **'Buyer'** in the RFP, unless repugnant to the context, refers to the Munitions India Limited (MIL) in the RFP.

10. The usage of the term **'Contract'** in the RFP, unless repugnant to the context, refers to the consequent Purchase Order / Supply Order/ Contract.

11. The Last Date of Submission of proposal is **23/12/2024**

12. **Procurement Approach:**

The procurement of IaaS Services from ISP to provide the Data Centre (also referred as DC) and Disaster Recovery (also referred as DR) set up for SAP S/4 HANA ERP Solution to MIL will consist of the following key activities.

(a) An invitation to submit and participate in the proposal will be sent to M/s RailTel Corporation of India through CPPP/E-mail. No other ISP is eligible to submit and participate against this RFP.

(b) The Bidder may visit MILCO and its Units for any clarification/understanding on any functional requirements, for which a request may be sent with details of personnel to visit unit(s) under MIL with their identity proof.

The Bidder is requested to fill the Form 6 for checklist of Documents for completeness of submission.

-Sd-

ED /Modernization & ERP

Munitions India Limited for CMD, MIL

1. OVERVIEW:

MIL is Defence Public Sector Enterprise (DPSE). MIL is India's largest manufacturer and market leader engaged in Production, Testing, Research & Development and Marketing of comprehensive range of Ammunition & Explosives for Army, Navy, and Air Force & Para-Military Forces in India. MIL in its 12 state-of-the-art manufacturing units located across the country has integrated base for production of Small, Medium & High Caliber Ammunition, Mortars, Rockets, Hand Grenades etc. with in-house manufacturing of Initiatory Compositions, Propellants and High Explosives for over 150 years. The primary objective of MIL is to provide competitive edge to the Armed Forces by equipping them with modern and quality battlefield Ammunition in pursuance of the 'Schemes and Programs' of the Government of India. MIL has significant patronage abroad including countries located in North America, South America, Europe, Africa and Asia, reflecting confidence in the quality of MIL products and services.

A Leadership team has been instituted to chart the create vision, set directions, and lead the transition into a self-reliant Public Sector Enterprise. The transition journey will necessitate changes to the current business processes and ways of working. One of the key identified areas to enable the transition has been "Enterprise-wide Resource Planning (ERP)" package which can integrate all processes into a single fully integrated system, ensure standardization, enable seamless flow of materials, money and information to relevant stakeholders and facilitate governance and effective decision making.

Munitions India Ltd (herein after referred to as **"MIL"),** has decided to setting up of Data Center & Disaster Recovery Center based on Infrastructure as a service (IaaS) Platform for SAP S/4 HANA ERP Solution.

Buyer is planning to engage M/s RailTel Corporation of India (herein after referred to as **"RailTel"**), the Infrastructure Service Provider (ISP) for the hosting of ERP applications at DC/DR, further to their Memorandum of Understanding (MoU) signed at MIL Pune on dated 16/04/2024.

Hereinafter, both "MIL" and "RailTel" will individually be referred to as "Party" and jointly as "Parties", as the context may require.

2. SECTION I: GENERAL INFORMATION

This RFP is invited as single tender enquiry on nomination basis and only M/s RailTel Corporation of India is eligible to participate in this RFP. Being a Single Tender Enquiry, the technical and financial terms will figure in the same bid and their evaluation, shall be done together.

It has been MIL's endeavour to include all the essential components for setting up a complete DC/DR and WAN MPLS, however in case the ISP feels that additional components will be required to run the installation smoothly as a complete solution the same shall be factored as part of the proposed solution.

2.1 Requirement of Techno-Commercial Proposal:

2.1.1 The Bidder is required to provide in the Techno-Commercial Proposal in detail of how the Bidder proposes to implement the DC/DR system based on Infrastructure as a Service (IaaS) Platform for the proposed Implementation and comply all the performance, physical security and the Cyber Security requirements.

2.1.2 Server Hardware Sizing for DC/DR is provided in Annexure A.

2.1.3 All Networking equipment required for communication between servers, storage quoted and with the LAN/ Firewall of MIL for both DC/DR site shall be treated as part of hardware and in the service scope of the Bidder.

2.1.4 The Bidder shall provide all necessary Hardware & Software for both DC/DR. Both DC/DR site will be in Active-Passive mode. DC is fully active, and the DR site is on standby. The DR site only becomes active during a failure of DC.

DC/DR shall have replication of data. Necessary data replication software between DC/DR shall be considered. In case of failure of either of the site, provision shall be available to copy incremental data to the failed site once the site becomes operational.

2.1.5 While the Bidder has the freedom in making any assumptions about the processes and functions of MIL while interpreting the details given in this RFP, such assumptions cannot be the basis for any different interpretation. MIL retains the right of the final say in the interpretation of the scope of the work in terms of the interpretation of the functions and processes of MIL.

2.1.6 The Bidder shall also provide the services of latest Document Management System (DMS) including File and Dak Management, Meeting Management and Record Management systems along with necessary implementation and training.

2.1.7 The Bidder shall also provide a Tokenless Digital Signature Solution to be used in the DC/DR set up along with necessary implementation and training.

2.2 Instructions and Conditions for Techno-Commercial Proposal:

2.2.1 The Techno-Commercial proposal shall contain a detailed description of how the Bidder will implement the DC/DR system for ERP solution for MIL. It shall articulate in detail how the Bidder's methodology, technical teams, the management expertise and specific capabilities required for the DC/DR setup which will be deployed to meet the requirements of MIL, Security and Cyber Security compliance as specified in this RFP.

2.2.2 The Bidder must agree to provide design and specifications for all IT & Non-IT Infrastructure requirements to run the ERP solution and related add-on components.

2.2.3 The Bidder must agree to provide the governance structure and implementation plan for setting up of the DC/DR.

2.2.4 The Techno-Commercial Proposals must be direct, concise, and complete. Any information not directly relevant to this RFP shall not be included in the proposal.

2.2.5 MIL is also open to any suggestions that the Bidder may want to render with respect to setting up of DC & DR for SAP S/4 HANA System for MIL, for supply and maintenance of the Hardware, Network, Security and other add on tools in light of their expertise or experience from similar agreement.

2.2.6 The Bidder is requested to number all the pages of the Proposal including the annexure and other attachments.

2.2.7 The Bidder shall provide SAP Certified Server hardware.

2.3 Other Instructions:

2.3.1 The Bidder shall check the specifications and shall satisfy himself of the suitability of the equipment/solution being offered and shall take full responsibility for the completeness, efficient operations and guarantee of specified output of the equipment/solution offered.

2.3.2 The rates quoted shall be exclusive of all taxes, duties, levies. Statutory duties such as GST, other taxes, if applicable, shall be indicated separately.

2.3.3 Prices shall be quoted entirely in Indian Rupees. No clauses for price fluctuations due to fluctuation of the Indian currency against any of foreign currency will be accepted during the period of the contract.

2.3.4 If any of the solution components is priced as embedded within the overall solution in the quoted price submitted by the Bidder, the Bidder cannot un-bundle it and price it separately during the period of the contract for the solution.

2.3.5 MIL reserves the right to procure the components/services listed in this RFP in whole or in part.

2.3.6 Basic prices quoted in the proposal must be firm and final and shall not be subject to any upward revision/modifications. No upward adjustment of the commercial price shall be made on account of any variations except for tax component as per prevailing Laws at the time of invoicing.

2.3.7 **Correction of Error:**

2.3.7.1 Bidder is advised to exercise adequate care in quoting the prices.

2.3.7.2 Arithmetic errors in proposals will be corrected as follows:

(i) In case of discrepancy between the amounts mentioned in figures and in words, lowest price mentioned shall governed.

(ii) In case of discrepancy between the cost quoted in the pricing summary sheet for a component and the total cost provided for the component in the detailed cost break up sheet, the detailed cost breaks up sheet for the component will be considered.

(iii) In case of discrepancy between the total price given for a line item / component and the calculated total price (number of units multiplied by the cost per unit for that line item), the total price given for a line item / component will be considered.

(iv) The amount stated in the commercial proposal, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall proposal price to rise, in which case the proposal price shall governed.

(v) The amount stated in the Commercial proposal will be adjusted by MIL in accordance with the above procedure for the correction of errors and shall be considered as binding upon the Bidder.

2.3.8 All costs incurred due to a delay of any sort, solely attributable to the Bidder, shall be borne by the Bidder.

2.3.9 MIL reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated within specified time frames.

2.3.10 **Price and Price information:**

2.3.10.1 Once a contract is signed with the Bidder, based on the price proposal, no adjustment of the contract price shall be made on account of any variations in costs of labour and materials or any other cost component affecting the total cost in fulfilling the obligations under the contract. Tax shall be as per Prevailing Rates during currency of the original contract period.

2.3.10.2 The Contract price arrived at, shall be the only payment, payable by MIL to the Bidder for completion of the contractual obligations by the Bidder under the Contract, subject to the terms of payment.

2.4 General Conditions of Contract:

2.4.1 Submission of Pre-Contract Integrity Pact along with the Bid failing which the bid is liable to be rejected.

2.4.2 Once a contract is signed with the Bidder, no adjustment of the Contract price shall be made on account of any variations in costs of labour and materials or any other cost component affecting the total cost in fulfilling the obligations under the contract.

2.4.3 During the period of the contract, MIL could buy any of those items which are not included in the contract, and which are part of the quote price of the Bidder. MIL will have the right to buy those services at the same rate. The commercial quote for all the services indicated in the quote will be valid for the complete period of the contract.

2.4.4 The Buyer reserves the right to reject/cancel/scrap the RFP or change the quantity of tendered item(s) without notifying any reason whatsoever.

2.5 Signing of tender:

(a) The tender shall be signed by a competent authority (digitally sign in case of e- procurement) holding power of attorney to handle such job on behalf of tendering bidder and this fact must be stated explicitly.
(b) Individual signing the tender or other documents connected with a contract must specify whether he signs as:
  (i) 'Sole Proprietor' of the bidder or constituted attorney of such Sole Proprietor.
  (ii) A partner of the bidder, if it be a partnership, in which case he must have authority to quote & to refer to arbitration dispute concerning the business of the partnership either by virtue of the partnership agreement or a power of attorney;
  (iii) Constituted attorney of the bidder if it is a company.
(c) In case of (a)(ii) above, a copy of the partnership agreement or general power of attorney, in either, case, attested by a Notary Public shall be furnished or affidavit on stamped paper of all the partners admitting execution of the partnership agreement or the general power of attorney shall be furnished.
(d) In case of the partnership bidders, where no authority to refer disputes concerning the business of the partnership has been conferred on any partner, the tender and all other related documents must be signed by every partner of the bidder.
(e) A person signing the tender form or any documents forming part of the contract on behalf of another shall be deemed to warrantee that he has authority to bind such other persons and if, on enquiry, it appears that the persons so signing had no authority to do so, the purchaser may, without

prejudice to other civil and criminal remedies, cancel the contract and hold the signatory liable for all costs and damages.

(f) In case of manual TE, each page of the tender, schedule to tender and Annexure, if any, shall be signed by the bidder.

2.6 **Queries & Clarification:**

Queries/clarifications of all nature, if any that may arise shall be referred by the Bidder by RFI (Request for Information) by Letter/email direct to the signatory at the following address:

ED/Modernization & ERP

Munitions India Limited

2nd Floor Nyati Unitree, Nagar Road,

Yerwada, Pune – 411006.

Contact: 020-67080400

Any queries/clarifications related to the RFP shall be sent to the following email addresses:

E-mail: modernization@munitionsindia.in

3. SECTION II: DETAILS OF THE ITEM/SERVICES REQUIRED

3.1 Data Center IT Infrastructure Requirements Specification:

MIL is planning to establish Data Center (DC) and Disaster Recovery Center (DR) with ISP as an Infrastructure Service Provider (ISP) agency for the hosting of ERP applications. These Data Centers will provide all the IT services to 17 locations of units under MIL in integrated manner. The proposed DC & DR site shall be within Geographical location of India. As part of the Business Continuity Plan the Disaster Recovery Center must be at different seismic zone in India. DC and DR will be interconnected asynchronously through the WAN connectivity provided by Bidder.

MIL is using Intranet (ComNet) network Infrastructure of RailTel MPLS WAN connectivity across all 16 locations. Additionally, the new location of New Delhi is to be added to this Network. MIL intends to use the existing network infrastructure of ComNet together with additional Routers and bandwidth.

3.1.1 Information about Geographical Locations of Units under MIL:

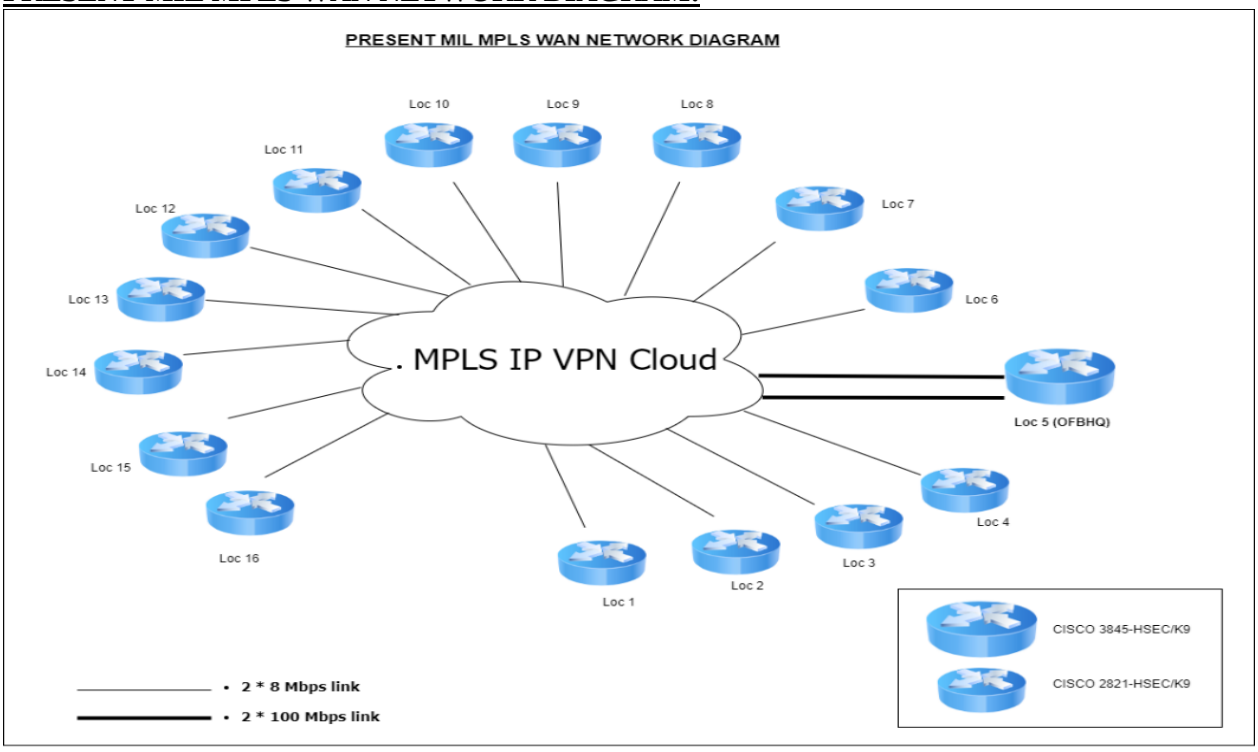
Units of MIL are using PCs that are connected in a Local Area Network (LAN) for all their Enterprise applications. These LANs have been integrated into WAN on MPLS Communication Network (COMNET 2.0) at 16 sites under MIL except Liasoning Office, New Delhi. All the locations under MIL are connected by RailTel backbone on MPLS in a hub and spoke architecture with the Central location at Directorate of Ordnance (Coordination & Services), Kolkata erstwhile OFB (Ordnance Factory Board). The entire network is managed by RailTel for DoO (C&S).

The Geographical locations of all units under MIL is given below:

Sr. No	Unit Name	Location	State	Code	Region
1	MIL Corporate office (ComNet connection from Mumbai Liaison office was shifted)	Pune	Maharashtra	MILCO	Western
2	Ammunition Factory	Khadki	Maharashtra	AFK	Western
3	Cordite Factory	Aruvankadu	Tamil Nadu	CFA	Southern
4	High Energy Projectile Factory	Trichy	Tamil Nadu	HEPF	Southern
5	High Explosive Factory	Khadki	Maharashtra	HEF	Western
6	Ordnance Factory Bhandara	Bhandara	Maharashtra	OFBA	Western
7	Ordnance Factory Bolangir	Bolangir	Maharashtra	OFBL	Eastern

8	Ordnance Factory Chandra-pur	Chandrapur	Maharashtra	OFCH	Western
9	Ordnance Factory Dehu Road	Dehu Road	Maharashtra	OFDR	Western
10	Ordnance Factory Itarsi	Itarsi	Maharashtra	OFI	Western
11	Ordnance Factory Khamaria	Khamaria	Madhya Pra-desh	OFK	Western
12	Ordnance Factory Nalanda	Nalanda	Bihar	OFN	Eastern
13	Ordnance Factory Varangaon	Varangaon	Maharashtra	OFV	Western
14	Ordnance Factory Institute of Learning	Khamaria	Maharashtra	OFILKH	Western
15	MIL Controllerate of Safety (ComNet extended from AFK)	Pune	Maharashtra	MILCOS	Western
16	National Academy of Defence Production	Ambhajari	Maharashtra	NADP	Western
17	Liaison Office at Delhi (No ComNet at present)	Delhi	Delhi NCR	LIAISON OF-FICE DELHI	Northern

PRESENT MIL MPLS WAN NETWORK DIAGRAM:



RFP specifies all the essential components for running a complete DC/DR, however in case the ISP

feels that additional components will be required to run the installation smoothly as a complete solution the same shall be factored in as a part of the proposed solution.

ISP shall not propose hybrid type of CPUs / Cores in a single server box and should not supply refurbished items.

The DR shall be deployed at 100% for Production Servers & for Development, Quality Assurance & Training Landscapes at reduced capacity as per "Server Hardware Sizing" given in Annexure-A.

ISP shall conduct disaster trial as mutually agreed between MIL and RailTel time to time at the interval of every six months of operation, wherein the Data Center has to be deactivated and complete operations shall be carried out from Disaster Recovery Centre. ISP shall plan all the activities to be carried out during the Disaster trial and issue a notice to the MIL at least two weeks before such a trial.

ISP shall clearly define the procedure for announcing disaster, based on the proposed DR solution. ISP shall also clearly specify the reasons due to which disaster is being announced along with the implications of disaster and the time frame required for migrating to DR and recovery of DC.

3.1.2 **Items Required at DC/DR:**

(a) ISP will be responsible for the following aspects with regard to Data Center (DC) & Disaster Recovery Center (DR).

Sr. No	Data Center (DC)	Disaster Recovery Center (DR)
1	Server Systems for SAP ERP solution	Server Systems for SAP ERP solution
2	Server Systems for Non- ERP solution	Server Systems for Non- ERP solution
3	Core Switch	Core Switch
~~4~~	SD-WAN Router	SD-WAN Router
5	Firewall & IPS (Intrusion Prevention System)	Firewall & IPS (Intrusion Prevention System)
6	SIEM - Security Information & Event Management	SIEM - Security Information & Event Management
~~7~~	Network Management Software	Network Management Software
8	Storage and Real-Time Backup Solution	Storage and Real-Time Backup Solution
9	Security Mechanism	Security Mechanism
10	Anti-virus Server/Client for all Servers	Anti-virus Server/Client for all Servers
11	8 Mbps MPLS Ports for 16 remote sites, 12 Mbps MPLS Port for New Delhi site and 140 Mbps Port at DC	140 Mbps Port at DR
12	Virtualization Software	Virtualization Software
13	Patch Management Software	
14	Internet Link of 10 Mbps with Router and Firewall	
15	Data Leak Prevention (DLP)	

(b) MIL 16 remote Locations to be connected to RailTel DC/DR with 8 Mbps MPLS (Multi-Protocol Labeled Switch) Bandwidth and New Location at Delhi with 12 Mbps MPLS Bandwidth along with SD-WAN (Software-Defined Wide Area Network)

3.1.3. **Storage and Real-Time Backup Solution:**

3.1.3.1 The backup and archival is proposed to be implemented at the DC/DR site. All the servers will have redundant data path to storage through multi-pathing software, redundant HBAs (Host Bus Adaptors) and redundant storage array. If any device in one path fails the data packets will be automatically re-routed through the other available path.

3.1.3.2 The Storage will be configured with the management software. At DC/DR, the solution requires multiple copies of the production volumes to be made within the storage array. For this functionality storage array will be configured with Business Continuance Volume / equivalent software.

3.1.3.3 The real-time replication used in this solution is storage based "Storage to Storage" replication between DC to DR Site. From the storage array the data moves through storage and multi-protocol router to WAN links. The replication mechanism will be achieved through a storage array Replication software.

3.1.3.4 Asynchronous Replication shall be deployed between DC and DR.

3.1.3.5 DR site is an important infrastructure where all the production information is generated and maintained by way of replication from the DC. If there is a disaster at the DC then the DR site will become operational.

3.1.3.6 **Backup Policies:**

Backup policy should take into consideration the factors like minimum permissible data loss, minimum recovery time, High data availability & actions should be taken in the event of backup failures and backup strategy that make sure zero impact on backups i.e., backups do not harm the performance of the database servers. With proper understanding of the business process and requirements, ISP shall define the backup policies and backup strategies.

3.1.3.7 **Backup Strategy:**

The sample backup strategy can be set as show below:

(a) Backup Type: Disk to Disk

(b) Backup Method (Incremental, Full)

(c) Backup Frequency (Daily, Weekly, Monthly)

(d) Backup Log (Daily, Weekly, Monthly)

(e) Retention Policy (Daily, Weekly, Monthly)

(f) Backup Monitoring and Reporting

Sr. No.	Description	Backup Type	Retention Type
1	Daily	Incremental backup	7 Days
2	Weekly	Full Backup	1 Month
3	Monthly	Full Backup	2 Months

3.1.3.8 **Backup Methodology:**

ISP should provide a detailed methodology for data backup, data monitoring and reporting. Below are the key expectations for the backup methodology.

(a) Storage Based Replication will be deployed to ensure zero data loss.

(b) Using Storage Based replication, the data will be replicated asynchronously from DC to DR Site.

(c) Restoration and testing of backup once in six months.

(d) Backup activities will be monitored on daily basis.

(e) Backup logs and activity/status logs will be checked on daily basis.

(f) Monitoring and status report will be maintained and submitted as & when required.

(g) Support for file and volume restoration requests if and when required.

3.1.4 **Data Center Management:**

Below will be the tasks and approach for the Data Center Management that should be done by the ISP:

3.1.4.1 Hardware Resource Monitoring: The administrator should monitor the Server, CPU, RAM, Storage and performance of the servers and Networking devices.

3.1.4.2 Auto-discovery of all Network devices and providing with their detailed configuration should be done by the ISP.

3.1.4.3 Uptime Report**:** The Current and Historical uptime report should be generated and shared periodically by the ISP.

3.1.4.4 IP Management**:** The ISP should reserve the dedicated IPs for servers.

3.1.4.5 OS Management: The ISP should provide the OS and make the necessary upgrade in it.

3.1.4.6 Rack Management and Monitoring**:** ISP should monitor the rack and devices mounted in the rack from single console.

3.1.4.7 Virtual Machine Management: The ISP should create, recycle, shutdown and reboot the VM remotely with prior permission from the MIL.

3.1.4.8 Bandwidth Monitoring: The ISP should monitor the input and output bandwidth.

3.1.4.9 Service Monitoring: This option enables to monitor the services running on the servers.

3.1.4.10 Syslog Monitoring: The ISP should monitor all type of logs, custom files and share it with MIL, in case it is required.

3.1.4.11 Alerts Notification: When the device goes down, it should send an alert notification via SMS / e-Mail to designated MIL personnel.

3.1.4.12 User Management (Admin):

(a) The ISP should ensure the creation of administrator account and giving permission to account in the system according to job profile of administrator.

(b) While creating a User ID, Password should be always generated. Password should be as per defined password policy.

(c) Access of user IDs should be reviewed periodically to cutoff additional access. Further actions like retaining the conflicting access with mitigating controls or removal of conflicts.

(d) Appropriate approvals should be taken prior to assigning sensitive/critical access.

(e) Parameters should be used to force users to change password periodically.

(f) Inactive users should be end dated and removed from system.

(g) Off boarded users should be terminated from the system landscape on the last day of their service.

(h) The ISP shall maintain access controls to protect and limit access to the authorized End Users of the MIL.

(i) The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users.

3.1.5 **Disaster Recovery:**

The Design & Operation of Disaster Recovery will be set up based on the following parameters:

(a) **RTO** (Recovery Time Objective): RTO is the maximum acceptable amount of time for restoring a network or application and regaining access to data after an unplanned disruption.

(b) **RPO** (Recovery Point Objective): RPO is maximum length of time permitted that data can be restored from, which may or may not mean data loss.

3.1.5.1 The principle of disaster recovery is that the data is kept in a DR Site as well as in backup system, and plans are made on how that data will be recovered so that the business becomes accessible again.

3.1.5.2 Disaster recovery (DR) is about preparing for and recovering from a disaster. Any event that has a negative impact on the business continuity or finances could be termed a disaster including hardware or software failure, network outage, power outage, physical damage to a building (such as fire or flooding) or even human error.

3.1.5.3 ISP is responsible for providing Disaster Recovery Services so as to ensure continuity of operations in the event of failure of Data Center and should meet the RPO and RTO requirements.

3.1.5.4 RPO would be 5 minutes and RTO would be 02 Hours. In case the DC environment goes down, the ISP shall scale up the DR environment for the services to be delivered without any effect on the performance.

3.1.5.5 DC production environment shall be replicated on an ongoing basis and shall be available as per designed RTO/RPO and the replication strategy.

3.1.5.6 In the event of a DC site fail-over or switchover, DR site will take over the active role, and all requests will be routed through DR site.

3.1.5.7 Whenever there is fail-over from DC to DR, production environment of DR site shall be equivalent to DC including all the security features and components of DC, without the fail-over components.

DR Scenarios:

Scenarios of Production Site failure:

(i) The 'DC' can be said to be down, whenever any of the equipment stop functioning as required leading to non-availability of servers hosting ERP Production Environment.

(ii) If DC is down due to 'failure of network connectivity' between the DC and 17 locations of MIL, the DR must become 'active' in such a way that 17 locations of MIL shall connect to DR.

(iii) If DC is down due to non-functioning of any of the 'DC Network Equipment's' or their internal components - the DR must become 'active' in such a way that 17 locations of MIL shall connect to DR.

(iv) The 'DC' can be said to be down, whenever any of the equipment's installed stop functioning as required. Illustratively.

(a) Fire accident at DC

(b) Auto shut down of DC servers irrespective of reasons for the same

(c) Natural disasters at DC

(d) Theft and damages due to human behaviour etc.

3.2 Network Infrastructure Requirements Specification:

3.2.1 System Integrator needs to plan Network layout and connectivity within the DC/DR and All 17 locations under MIL. The IP addressing scheme for all implementation locations will be worked out by ISP. ISP is expected to ensure compatibility between various network components of MIL & COMNET WAN. ISP will liaise with Network Administrator of MIL for ensuring compatibility between various network components of DC/DR and COMNET WAN.

3.2.2 Brief Description of the Other Major Items at DC/DR:

3.2.2.1 Firewall & IPS

The Firewall+IPS should be single unit based which should have multi-Gig performance, will have application visibility and security features.

Both the Firewall and IPS should have Gig Interfaces capability. ISP shall implement IPS at all the critical network points, both internal and external, for monitoring and addressing the unauthorized access attempts and the malicious activities in the network.

3.2.2.2 Core Switch

Switch with redundant management module and redundant Power supply Unit PSU on single box to connect both switches in high availability mode. Hot-swappable line cards, management modules, power supplies, and redundant fan with both the management modules in active condition to share the load. Both the core switches at DC should share single configuration file for automatic fail over even for inter VLAN routing tables.

3.2.2.3 **Data Leak Prevention (DLP)**

DLP is the practice of detecting and preventing data breaches, ex-filtration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations. DLP is to identify and prevent the unauthorized sharing, transfer, or misuse of sensitive data within an organization, helping to protect against data breaches.

(a) The solution shall have a dashboard showing details of current activity with the organization from DLP point of view. The DLP system should be able to provide detailed view of each of the components in DLP system like the agent scanning status, network appliance status and incident status etc.

(b) The solution shall have extensive reporting and auditing capabilities. The solution shall provide customized reports and notifications.

(c) The solution shall provide incident notification as well as escalation workflows for unattended incidents. The incident workflow should be configurable for each policy that is configured within the DLP system.

3.2.2.4 Network Management Software to maintain Switches and Routers Should be able to monitor and manage the Switches, security and Routers across the network.

3.2.2.5 Bandwidth for ERP solution to be considered as 8 Mbps at 16 locations and aadditionally, 12 Mbps at the new location of New Delhi.

3.2.2.6 Requirement of additional bandwidth will be provided by the ISP as per the requirement of MIL at any location at additional cost.

3.2.2.7 Addition of new location to MIL will be considered for WAN MPLS by the ISP if the new location is feasible.

3.2.2.8 Internet Bandwidth for Patch Management etc. is to be considered as 10 Mbps with Router and Firewall at DC.

The Bidder needs to provide the infrastructure details having below details.

Sr. No	Details
1	The proposed DC & DR site should be located within Geographical location of India.
2	The DC & DR must be in a different seismic zone.

3	The Data Centre and associated services must be ISO 20000 and ISO 27001 certified. Certified for Tier-III (Design & Facility). ISO 27001:2022-Certified for Information Security Management System, ISO 20000-1:2018 Certified for Information Technology Service Management System, ISO 9001:2015 Certified for Quality Management System, ISO 27017:2015 Certified for Information Security for Cloud Services and ISO 27018:2019 Certified for Data Privacy in Cloud Service.
4	The Data Center should have required different zone security layer.
5	The backup power generators should be N+N.
6	ISP should comply with all the Meity guidelines and should be Meity empanelled Cloud Service Provider.
7	ISP should carry out Cyber Security audit of DC/DR through CERT-IN empanelled auditors on every year basis, however first audit should be carried out before Go-Live of ERP.

3.3 **Contract Period:**

The contract will be awarded for a period of six (6) Years beginning from the declaration of Go-Live of the DC/DR set up. This contract can be further extended on the same terms for an additional period of Three (3) years. Upon the expiry of the contract period and /or the extended period the contract can further renewed on same terms with mutual agreement.

4. SECTION III: SCOPE OF WORK

Bidder will provide the required hardware, its associated accessories and software component for the DC/DR setup. ISP will provide the checklist for successful UAT (User Acceptance Test) acceptance of Hardware. Production, Non-Production, Development, Quality and Training platforms.

ISP shall agree to provide details about Design setup of DC/DR covering all aspects of network – the physical topology, protocol architectural, configuration parameters and the respective service descriptions. Also, ISP shall agree to provide technical operation manual in hard and soft copy format to MIL.

4.1 Security Mechanism:

4.1.1 Physical Security at the Data Center:

ISP should made provision of multiple level of physical security in its Data Center. Multiple levels of authentication are required in order to reach to MIL's IT infrastructure equipment. Motion-based cameras should monitor every corner of building and inside of data center along with security guards and Building Management Services team.

Following outlines, the multiple level security that should be provided by the ISP for DC-DR facilities:

4.1.1.1 Bio-metric and Proximity Card Access Control System to all doors:

ISP IDC should be secured by multiple levels of security systems, one of them being Bio-metric access control unit. These devices should be installed on each door. In addition to this, Proximity Card Access Control System has to be installed on DC Main entrance gate and Support floor.

4.1.1.2 Separation of MDA room and Server Area with different Access Level:

Main Distribution Area room should be separated from the Data Centre room where MIL's IT infrastructure equipment have been installed. Both rooms should have bio-metric access control facility installed. Server room will be accessible by all the Network Engineers from Network Operations Center, while MDA room access is restricted to all except higher technical authorities such as Network Administrators and Managers.

4.1.1.3 Control access Rack:

ISP should have installed some rows of racks which have mechanical key lock system or Bio-metric system to provide added security.

4.1.1.4 Video Surveillance System:

ISP Data Center building and surrounding should be monitored using Video surveillance system installed. Main entrances, pathways, corridor, Reception lobby, Parking areas, Data Center, NOC room should be continuously monitored 24x7 using CCTV Cameras. The video taken by these cameras monitored by security personnel

and these video clips should be retained for minimum 3 months.

4.1.2 **Network Security at the Data Center:**

4.1.2.1 **External Firewall:**

(i) External Firewall/UTM with IPS capabilities should be proposed at Perimeter zone at the DC site to protect MIL Infrastructure zone from the 17 locations of MIL and Internet traffic.

4.1.2.2 **Intrusion Prevention System – IPS:**

(i) The Proposed Integrated IPS solution with the Firewalls delivers throughput in Gbps to protect networks from both known and unknown threats. IPS offers a wide range of features that can be used to monitor and block malicious network activity including predefined and custom signatures, protocol decoders, packet logging, and IPS sensors.

(ii) The IPS solution will be integrated with the Firewall to support inspection of many protocols in one unified system.

4.1.2.3 **Security Information & Event Management - SIEM:**

The proposed Security Information & Event Management (SIEM) solution should be scalable solution for log management and IT compliance. SIEM should enables monitoring security tools and finding a correlation between them in real time as well as historically.

SIEM allows capture of log data as well as management and monitoring on the collected data. Appropriate event sources will be configured to send log data to the SIEM appliance for alerting and reporting.
SIEM provides,

(a) Security Monitoring

(b) Incident Investigation

(c) Compliance Reporting

(i) SIEM is a security solution that helps security analysts detect and investigate threats that are often missed by other security tools. By combining big data security data collection, management, and analysis capabilities with full network and log-based visibility and automated threat intelligence, security analysts can better detect, investigate, and understand threats they could often not easily see or understand before. Ultimately this improved visibility.

(ii) Collecting and storing logs from DC and DR devices is the primary function. These logs should be indexed with appropriate solution to make them easy search-

able even at high events per second (EPS). SIEM architecture should enable correlating multiple devices together irrespective of the fields present.

(iii) SIEM should enable finding root cause and abnormal behaviour by looking at the trends over time. In case of any attacks or potential attacks enables the security analyst to identify the root cause to ensure it is not repeated again.

(iv) SIEM deployment should be done at DC site (for centralized network logging, analytic, forensics and reporting and delivering increased knowledge of security events throughout the network).

(v) SIEM platforms should integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout the network.

(vi) The solution should provide network-wide reporting of events, activities, and trends occurring on all devices & provides centralized Logging of Multiple Record Types Including traffic activity, system events, & attacks.

(vii) The Network Event Correlation module should allow IT administrators to quickly identify and react to network security threats across the network.

(viii) It should Secure data aggregation from security infrastructure provides network-wide viability and compliance.

(ix) It should provide reports and customizable charts to monitor and maintain identify patterns, acceptable use policies, and demonstrate policy compliance.

(x) Online Logs and Offline logs will be retained for a minimum of 30 days.

4.2.2.4 **Anti-virus for Servers:**

The proposed solution should include the enterprise level anti-virus which will be installed on every virtual instance to prevent the instance from threats. Advanced Security and Management for all devices. Antivirus should provide unified threat protection and device management for servers to quickly protect all of endpoints from ransom-ware, zero-day threats and other sophisticated attacks.

4.2.2.5 **Data Leak Prevention – DLP:**

The proposed Data Leak Prevention (DLP) solution should be proposed at Perimeter zone at the DC site to discover, classify, monitor and protect MIL data from external and internal network.

4.3 **Managed Services for DC/DR:**

DC and DR will be managed by an internal Network Operations Center (NOC) and support teams of ISP with various in-house developed tools which is a complete Data Center Management Tool.

(i) Managed Services for Servers, Storage, Switches, Routers, Networking Devices, Firewall, Security Components, except application support.

(ii) Data Center Uptime Management

(iii) Server Administration & Management

(iv) Storage Administration & Management

(v) Network Administration & Management

(vi) Security Administration & Management

(vii) Virtualization / Physical environment Management

(viii) Windows / Linux Operating System Administration & Management

(ix) Antivirus Administration & Management

(x) Backup/Restore Administration & Management for Servers, Database, and Applications etc.

(xi) Configuration, administration, customization, upgrade, patch management, new release deployment.

(xii) Preventive Maintenance

(xiii) Reporting & Documentation

(xiv) Call Logging and Help Desk Management

(xv) Security Operation Center (SOC)

4.3.1 **Support Service for the Infrastructure Hosting:**

The Support should be available through Web portal, Phone and Email. The speed and reliability of the resolution process is hence critical to the MIL's reputation.

4.3.2 **Logging Calls with Online Helpdesk:**

(i) An Industry standard Online Helpdesk monitored by support personnel 24x7.

(ii) MIL can log a call by contacting ISP Online Helpdesk/Support department through phone, email or live chat.

(iii) ISP Helpdesk/Support team should then check the problem and perform Level 1 troubleshooting.

(iv) Once the issue is resolved, user can confirm by responding to the associated ticket raised through online helpdesk by giving feedback.

(v) Escalation matrix needs to be provided for any delay in resolution of call log.

Email and mobile access must be provided.

4.3.3 **Incident Management and Support Strategy:**

Incidents can be formally communicated through ticket or E-Mail. If the call is logged via email, then the Ticket will be generated and automatically sent to the Customer.

If call is logged using Phone or Chat, ISP support Team should log the incident in the Helpdesk portal.

Help Desk team should respond to the incident by calling the user directly to get the detailed problem and trying to resolve the issue over phone, if not then assign an Engineer to resolve the call.

Incidents are classified based on severity to ensure that the response is appropriate to the severity of the issue. A detailed definition for each of these severity levels, together with the proposed acknowledgment time and action required should be provided by the ISP in its proposal.

4.3.4 **24 x 7 Support" Over email, Ticket, Phone & Online Chat:**

ISP' Support Staff will be available 24 x **7** for any support related to the services provided. The Support team will maintain and monitor ISP's NOC and SOC and provide assistance to the customers at all times. The Support Team can be reached through the Client through telephone, email or online chat.

4.3.5 **Response Time with Resolution Matrix:**

Response time is defined as the time between receipt of the incident by support team and its logging/generation of ticket on the system.

Resolution Time shall mean the time taken (after the incident has been reported to the support team) till resolution. The severity parameters have been defined below:

The Severity would be as follows:

(a) **Critical:** Services are not available.

(b) **High:** Services are available partially.

(c) **Medium:** Services available however response time is slow/poor.

(d) **Low:** Service requires upgradation with or without downtime.

Maximum time to Log the Call:

Severity Level	Production Environment	Non-Production Environment	Replication	Backup	MPLS and Network at DC/DR site	MPLS and Network at Client Location
Critical	15 min	30 min	15 min	15 min	15 min	15 min
High	30 min	60 min	30 min	30 min	30 min	30 min
Medium	45 min	90 min	45 min	45 min	45 min	45 min
Low	60 min	120 min	60 min	60 min	60 min	60 min

Maximum time to Restore/Resolve the Logged Call:

Severity Level	Production Environment	Non-Production Environment	Replication	Backup	MPLS and Network at DC/DR site	MPLS and Network at Client Location
Critical	2 Hours	4 Hours	2 Hours	2 Hours	2 Hours	2 Hours
High	4 Hours	6 Hours	4 Hours	4 Hours	4 Hours	4 Hours
Medium	6 Hours	8 Hours	6 Hours	6 Hours	6 Hours	6 Hours
Low	8 Hours	10 Hours	8 Hours	8 Hours	8 Hours	8 Hours

The ISP shall provide business continuity and disaster recovery services to meet the RPO and RTO. The following should be followed:

Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) Change over from DC to DR or vice versa.	RTO <= 2 hours
Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) change over from DC to DR or vice versa.	RPO <= 5 minutes

4.4 Roles and Responsibilities:

4.4.1 Infrastructure Service Provider (ISP):

Following are the responsibilities of the ISP:

(i) The ISP shall be responsible for provisioning the underlying System, software, Infrastructure, and Infrastructure Services for deployment of ERP on the Infrastructure in the form of "Infrastructure as a Service" (IaaS).

(ii) The ISP in coordination with MIL shall be responsible for adequately sizing of the necessary compute, memory, and storage required to build the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.

(iii) The ISP shall be responsible for provisioning the necessary Compute, Memory, and Storage as per the recommendations of the MIL.

(iv) The ISP shall coordinate with the MIL for hosting of applications and migration of data on the infrastructure in the form of "Infrastructure as a Service" (IaaS).

(v) The ISP Shall coordinate with MIL and its SI for hosting of ERP, Planvisage and ITSM System and any other applications commissioned by Client for meeting their requirements.

(vi) The ISP shall specify/confirm RTO, RPO, clustering/high availability, proposed application uptime, proposed application response time for all applications and their respective storage requirements.

4.4.2 **Client – MIL:**

(i) The MIL and its SI shall coordinate with the ISP for hosting of applications and migration of data on the infrastructure in the form of "Infrastructure as a Service" (IaaS).
Below are the roles and responsibility matrix that need to be complied by all the stakeholders

Note: R: Responsible A: Accountable C: Consulted I: Informed

Activity	MIL	SI/Client Nominated Agency	RailTel
Provisioning and Installation			
Infrastructure Setup	I	C	R/A
Provision of Rack Space Power & Cooling	I	C	R/A
Server Racking, Stacking, and Console Network Configuration.	I	C	R/A
Provision of Server, Network & Security Component	I	C	R/A
Operating System Installation and Configuration	I	C	R/A
WAN Link Provisioning & Installation	I	C	R/A
Network & Security Devices Installation, Configuration.	I	C	R/A
P2P Replication Link Provision	I	C	R/A
Database Fail-over Cluster Configuration	I	R/A	C
Application Installation, Configuration, & Implementation	I	R/A	C
Database Installation, Configuration & Implementation	I	R/A	C
License Provisioning			

Operating System	I	C	R/A
Virtualisation Software	I	C	R/A
Application license (SAP ERP system, ITSM, Planvisage)	I	R/A	C
Database License for SAP ERP system	I	R/A	C
Database License for ITSM and Planvisage	I	R/A	C
Operations and Management			
Operating System Administration & Day to Day Management & Troubleshooting	I	C	R/A
User Access Management	R/A	C	C
Server & Storage Management	I	C	R/A
Firewall Management	I	-	R/A
Network Management	I	-	R/A
Backup Management	I	C	R/A
Management & Troubleshooting	C	C	R/A
Security Stack Management	I	-	R/A
WAN Link Management	I	-	R/A
P2P Replication Link Management	I	-	R/A
Network & Security Devices Management.	I	-	R/A
Database Fail-over Cluster Management	I	R/A	C
24 x 7 L1/L2/L3 Support	I	C	R/A
ERP Application, Database Migration	R	A	C
Any OS Level Migration	I	C	R/A
Application Basis Support & Management	R	A	C
Application Cluster Management	I	C	R/A
Database Cluster Management (HANA)	I	R/A	C
Application Day to Day Management & Troubleshooting & Other Database Day to Day Management & Troubleshooting	I	R/A	C
Other Application Migration	I	R/A	C
Other Database Migration	I	R/A	C
Backup Testing on The Test Environment	I	C	R/A
Upgradation of resources to meet the Performance	I	C	R/A
Replication Monitoring & Management	I	C	R/A
DR Drill (Once in 6 months)	I/C	I/C	R/A
Upgradation of resources to meet the performance	I	C	R/A
Patch Management			

Operating System Patch Management	I	C	R/A
Virtualization nodes patch Management	I	C	R/A
Application Patch Updating & Testing	I	R/A	C
Data Base Patch Updating & Testing	I	R/A	C
Planvisage Patch Updating & Testing	I	R/A	C
Anti-Virus/Switch/Firewall/UTM Patch Management	I	C	R/A

4.5 Service Level Agreement:

4.5.1 Purpose:

This section describes the Service Levels to be established for the Services offered by the ISP to Buyer. The ISP shall monitor and maintain the stated service levels to provide quality service to Buyer.

The purpose of Service Levels is to define the levels of service provided by the Infrastructure Service Provider (ISP) to Munitions India Limited (MIL) for the duration of the contract.

4.5.2 General Principles of Service Level Agreement:

Service Level Agreement (SLA)

Service Level Agreement (SLA) shall become the part of the Contract between the MIL and the ISP. SLA defines the terms of ISP's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The ISP shall comply with the SLAs to ensure adherence to availability of quality service throughout the duration of the Contract.

4.5.3 Service Levels Monitoring:

The Service Level parameters shall be monitored on a quarterly/Instance basis.

As part of the DC/DR setup requirements, ISP shall supply and make sure of appropriate system (software/hardware) and Services to automate the procedure of monitoring SLAs during the course of the Contract and submit reports on quarterly/Instance basis for all SLAs as mentioned in this section.

ISP will follow instruction only from authorized personnel of the MIL.

For issues i.e., each of SLAs beyond control of the ISP, the ISP shall submit a justification for the consideration of the MIL.

4.5.4 **Measurement Targets & Penalties:**

Two types of penalties will be imposed mentioned as hereunder;

A] Penalty for delay in Installation & Commissioning :

In line with Cl.No. 4.6 (Delivery Schedule), the Bidder shall complete Installation & Commissioning of all IT Infrastructure at DC/DR and 17 locations within 04 (Four) months from the date of signing the Contract.

However, delay in completion of Installation & Commissioning, beyond the period of 04(four) months, shall attract penalty of Rs. 50,000/- per week, thereafter.

Installation & Commissioning	Penalty (Weekly Basis) In INR
Within 4 months	No Penalty
Dealy of every week beyond scheduled 4 months	Rs. 50,000/- per week.

B] Penalty Post Implementation Phase and during Operation Phase :

These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the Operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non- performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.

The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as a part of this section of the Contract.

ISP's published SLAs and penalties shall also be applicable during the course of the Contract.

Penalty on Non-adherence to SLA for DC and DR:

Uptime % (Quarterly Basis)	Penalty (Quarterly Basis) In INR
Equal to and above 99.982%	No Penalty
99.5% < = Availability < 99.982%	On Quarterly basis, Rs 20,000/-
99.0% < = Availability < 99.5%	On Quarterly basis, Rs 30,000/-
98.5% < = Availability < 99.0%	On Quarterly basis, Rs 40,000/-
98.0% < = Availability < 98.5%	On Quarterly basis, Rs 50,000/-
Availability < 98.0%	On Quarterly basis, Rs 1,00,000/- and will entitle MIL to discuss/terminate the contract/PO.

Penalty on Non-adherence to SLA for MPLS WAN Network:

Uptime % (Quarterly Basis)	Penalty (Quarterly Basis) In INR
Equal to and above 99.5%	No Penalty
99.0% < = Availability < 99.5%	On Quarterly basis, Rs 10,000/-
98.5% < = Availability < 99.0%	On Quarterly basis, Rs 15,000/-
98.0% < = Availability < 98.5%	On Quarterly basis, Rs 20,000/-
97.5% < = Availability < 98.0%	On Quarterly basis, Rs 25,000/-
Availability < 97.5%	On Quarterly basis, Rs 50,000/- and will entitle MIL to discuss/terminate the contract/PO.

Penalty on Non-adherence to SLA for Recovery Time Objective (RTO <= 2 hours):

RTO In Hours (For Each Instance)	Penalty (For Each Instance) In INR
Equal to and below 2 Hours	No Penalty
Between 2 Hours to 4 Hours	Rs 50,000/-
Between 4 Hours to 6 Hours	Rs 75,000/-
Between 6 Hours to 8 Hours	Rs 100,000/-
Between 8 Hours to 10 Hours	Rs 150,000/-
Above 10 Hours	Rs 300,000/-

Penalty on Non-adherence to SLA for Recovery Point Objective (RPO <= 5 minutes):

RPO In Minutes (For Each Instance)	Penalty (For Each Instance) In INR
Equal to and below 5 Minutes	No Penalty
Between 5 Minutes to 30 Minutes	Rs 50,000/-
Between 30 Minutes to 60 Minutes	Rs 75,000/-
Between 60 Minutes to 75 Minutes	Rs 100,000/-
Between 75 Minutes to 90 Minutes	Rs 150,000/-
Above 90 Minutes	Rs 300,000/-

Severity of Helpdesk and issue response and resolution related SLAs will be as per following:

Penalty per Hour Exceeded beyond SLA Resolution Time (Rs. /Incident):

Severity Level	Penalty (Rs. /Incident)
Critical	Rs. 5000/-
High	Rs. 4000/-
Medium	Rs. 3000/-
Low	Rs. 2000/-

4.5.5 **Reporting Procedures:**

ISP representative shall prepare and distribute "Service Level Performance" reports in a mutually agreed format **along with the Invoice or upon request of the Client**. The reports shall include **"actual versus target"** Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be submitted to MIL.

4.6 **Delivery Schedule:**

4.6.1 The Bidder shall complete Installation & Commissioning of all IT Infrastructure at DC/DR and 17 locations within 04 (Four) months from the date of signing the Contract.

4.6.2 The Bidder is requested to provide Monthly Progress report to MIL on Installation & Commissioning of IT Infrastructure at DC/DR & 17 locations.

4.6.3 The Bidder will submit the notice of readiness to MIL to initiate the Installation of the ERP Solutions. After receiving notice of readiness from ISP on the setting up of DC/DR, MIL will intimate to SI of ERP for Installation of ERP solution. Then SI will initiate the Installation of ERP with the help of RailTel team and complete the same within 30 days of receiving intimation from MIL.ISP will carry out CERT-In audit after completion of all the activities before Go-Live of ERP Solution and then issue the notice of readiness for Go-Live.

5. SECTION IV: STANDARD CONDITIONS OF RFP

The Bidder is required to give confirmation of their acceptance of the Standard Conditions of the Request for Proposal mentioned below which will automatically be considered as a part of the Contract.

5.1 Law:

The Contract shall be considered and made in accordance with the laws of the Republic of India. The Contract shall be governed by and interpreted in accordance with the laws of the Republic of India.

5.2 Effective Date of the Contract:

5.2.1 The Contract shall come into effect on the date of signatures of both the parties on the Contract (Effective Date)

5.2.2 The Contract shall remain valid until the completion of the obligations of the parties under the Contract. The deliveries and performance of the services shall commence from the effective date of the Contract.

5.3 Dispute Resolution:

5.3.1 The Parties agree that the laws of India will govern this Contract.

5.3.2 At the first instance all the disputes or claim concerning the interpretation or application of the Contract signed between MIL and RailTel shall be settled amicably by mutual discussions between the authorized representatives of the Parties.

5.3.3 In the event that any dispute or difference relating to the interpretation and application of the provisions of this Contract is not settled amicably, such dispute or difference shall be taken up by either party for resolution through AMRCD as mentioned in DPE OM No. 05/0003/2019-FTS-10937 dated 14/12/2022 as amended from time to time, and the decision of AMRCD on the said dispute shall be binding on both the parties.

5.3.4 The Parties shall not be released from performing their obligations hereunder by reason of any dispute resolution proceedings being instituted.

5.4 Penalty for use of Undue influence:

The Bidder undertakes that he has not given, offered or promised to give, directly or indirectly, any gift, consideration, reward, commission, fees, brokerage or inducement to any person in service of the Buyer or otherwise in procuring the Contracts or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of the present Contract or any other Contract with the Government of India for showing or forbearing to show favour or disfavour to any person in relation to the present Contract or any other Contract with the Government of India. Any breach of the aforesaid undertaking by the Bidder or any one employed by him or acting on his behalf (whether with or without the knowledge of the Bidder) or the commission of any offers by the Bidder or

anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the Buyer to cancel the Contract and all or any other Contracts with the Bidder and recover from the Bidder the amount of any loss arising from such cancellation. A decision of the Buyer or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Bidder. Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the Bidder towards any officer/employee of the Buyer or to any other person in a potion to influence any officer/employee of the Buyer for showing any favour in relation to this or any other Contract, shall render the Bidder to such liability/ penalty as the Buyer may deem proper, including but not limited to termination of the Contract, importation of penal damages, forfeiture of the Bank Guarantee and refund of the amounts paid by the Buyer.

5.5 **Agents / Agency Commission:**

The Bidder confirms and declares to the Buyer that the Bidder is the original manufacturer of the stores/provider of the services or authorized by the OEM referred to in this Contract and has not engaged any individual or firm, whether Indian or foreign whatsoever, to intercede, facilitate or in any way to recommend to the Government of India or any of its functionaries, whether officially or un-officially, to the award of the Contract to the Bidder; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such interception, facilitation or recommendation. The Bidder agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in any way incorrect or if at a later stage it is discovered by the Buyer that the Bidder has engaged any such individual/firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this Contract, the Bidder will be liable to refund that amount to the Buyer. The Bidder will also be debarred from entering into any supply Contract with the Government of India for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract either wholly or in part, without any entitlement or compensation to the Bidder who shall in such an event be liable to refund all payments made by the Buyer in terms of the Contract along with interest at the rate of 2% per annum above LIBOR rate. The Buyer will also have the right to recover any such amount from any Contracts concluded earlier with the Government of India.

5.6 **Access to Books of Accounts:**

In case it is found to the satisfaction of the Buyer that the Bidder has engaged an Agent or paid commission or influenced any person to obtain the Contract as described in clauses relating to Agents/Agency Commission and penalty for use of undue influence, the Bidder, on a specific request of the Buyer, shall provide necessary information/ inspection of the relevant financial documents/information. The audit shall occur in a manner as deemed by the BUYER in each calendar year and shall be conducted expeditiously, efficiently, and at reasonable business hours. The Buyer shall not have access to the proprietary data of, or relating to, any other customer of the Bidder, or a third party or the Bidder's cost, profit, discount and pricing data, without the prior approval of. The audit shall not be permitted if it interferes with the Bidder's ability to perform the services in accordance with the service levels, unless the Buyer relieves the Bidder from meeting the applicable service levels.

5.7 **Non-Disclosure of Contract Documents:**

Except with the written consent of the Buyer/Bidder, other party shall not disclose the Contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party.

5.8 **Termination of Contract:**

5.8.1 The Buyer shall have the right to terminate this Contract in part or in full in any of the following cases: -

5.8.1.1 Events of default by ISP.

5.8.1.2 When the items offered by Bidder repeatedly fails in the inspection and/or Bidder is not in the position to either rectify the defects or offer items conforming to the Contracted to the quality standards.

5.8.1.3 When Bidder fails to honour any part of Contract including failure to deliver the Contracted stores/render services in time.

5.8.1.4 Unbranded/deceptively branded/ spurious supply against branded order in the Purchase Order.

5.8.1.5 When the Bidder is found to have made any false or fraudulent declaration or to statement to get the Contract or he is found to be indulging in unethical unfair trade practices.

5.8.1.6 Based on the decision of AMRCD.

5.8.1.7 By giving a notice of 01-month period.

5.8.2 **Termination Procedure:**

The Party entitled to terminate this Contract either on account of a Force Majeure Event or on account of an Event of Default shall do so by issue of a notice in writing to the other Party. The Termination Notice shall be of one month, ("Termination Period") and at the expiry of the Termination Period, this Contract shall stand terminated without any further notice.

5.8.3 **Obligations during the Termination:**

During Termination Period, ISP shall, subject where applicable to the provisions of this Contract, continue to perform such of their respective obligations under this Contract which are capable of being performed with the object, as far as possible, of ensuring continued availability of the DC/DR and services to the BUYER, failing which the ISP shall compensate the BUYER for any loss or damage occasioned or suffered on account of the underlying failure/breach.

5.8.4 **Termination Consequences:**

5.8.4.1 "The Liability of a Buyer in case of termination of the Contract initiated on account of Buyer in event of default shall be subject to a reasonable payment as MIL

deems fit and in case of event of default of Force Majeure, the liability shall be limited to full payments for Equipment, Systems, Licensed Software, up to the milestone immediately preceding the milestone ISP would be working on at the time of termination."

5.8.4.2 In case of termination due to ISP event of default, ISP shall pay damages amounting to encasement of all bank guarantees by BUYER and all outstanding payments. Any additional expenditure arising from subsequent negotiations of the Contract with any other agency will also be ISP's liability. Final payment up to the last completed milestone will be after handing over the complete documentation and meeting all requirements as per the Contract to the satisfaction of BUYER.

5.8.4.3 In the event of a termination effected in pursuance of this Contract, or expiry of this Contract, the relevant provisions of the Exit Management shall apply.

5.9 **Notices:**

Any notice required or permitted by the Contract shall be written in the English language and may be delivered personally or may be sent by registered pre-paid mail/airmail, addressed to the last known address of the party to whom it is sent.

5.10 **Transfer and Sub-letting:**

The Bidder has no right to give, bargain, sell, assign, or sublet or otherwise dispose of the Contract or any part thereof, as well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.

5.11 **Patents and other Industrial Property Rights:**

The prices stated in the present Contract shall be deemed to include all amounts payable for the use of patents, copyrights, registered charges, trademarks and payments for any other industrial property rights. The Bidder shall indemnify the Buyer against all claims from a third party at any time on account of the infringement of any or all the rights mentioned in the previous paragraphs, whether such claims arise in respect of manufacture or use.

5.12 **Amendments:**

The Provision of present Contract shall be changed or modified in any way (including this provision) either in whole or in part except by an instrument in writing made after the date of this Contract, mutually agreed and signed on behalf of both the parties and which expressly states to amend the present Contract without any financial implications or detoriation of service conditions for the buyer. Any such amendment will impact only the relevant referred sections of the contract with no derived implications on the rest of the contract.

5.13 **Severability:**

If any term or provision or clause of the Agreement (to be executed under this RFP) is declared invalid, illegal or unenforceable to any person the remainder of this Agreement shall be unimpaired and the invalid, illegal or unenforceable term or provision shall be replaced by such valid

term or provision as comes closest to the intention underlying the invalid term or provision and that term or provision shall be enforced to the fullest extent permitted by law.

5.14 **Taxes and Duties:**

5.14.1 If the Bidder desires to ask for GST, Sales Tax / VAT extra, the same must be specifically stated. In the absence of any such stipulation, it will be presumed that the prices include all such charges and no claim for the same will be entertained.

5.14.2 If reimbursement of any Duty/Tax is intended as extra over the quoted prices, the ISP must specifically say so. In the absence of any such stipulation it will be presumed that the prices quoted are firm and final and no claim on account of such duty/tax will be entrained after the opening of proposal.

5.14.3 If the ISP chooses to quote a price inclusive of any duty/tax and does not confirm inclusive of such duty/tax so included is firm and final, he shall clearly indicate the rate of such duty/tax and quantum of such duty/tax included in the price. Failure to do so may result in ignoring such offers summarily.

5.14.4 If ISP is exempted from payment of any duty/tax up to any value of supplies from them, He/she shall clearly state that no such duty/tax will be charged by him up to the limit of exemption which he may have. If any concern is available in regard to rate/quantum of any Duty/tax, it shall be brought out clearly. Stipulations like, the said duty/tax was presently not applicable but the same will be charged if it becomes livable later on, will not be accepted unless in such cases it is clearly stated by a Bidder that such duty/tax will not be charged by him even if the same becomes applicable later on.

5.14.5 Any change in any duty/tax upward/downward as a result of any statutory variation in GST etc. taking place within Contract terms shall be allowed to the extent of actual quantum of such duty/tax paid by the supplier. Similarly, in case of downward revision in any duty/tax, the actual quantum of reduction of such duty/tax shall be reimbursed to the Buyer by the Bidder. All such adjustments shall include all reliefs, exemptions, rebates, concern, if any obtained by the Bidder.

5.15 **Pre-Contract Integrity Pact:**

An “Integrity Pact” would be signed between the Buyer and the Bidder for purchases exceeding Rs5 crores, as follows.

An “Integrity Pact” would be signed between the Buyer and the Bidder for purchases exceeding Rs.5 Crs. Each page of such Integrity pact proforma would be duly signed by Purchaser's competent signatory at the time of issue of tender. All pages of the Integrity Pact are to be returned by the bidder (along with the technical bid) duly signed by the same signatory who signed the bid, i.e. who is duly authorized to sign the bid and to make binding commitments on behalf of his company. **Any bid not accompanied by Integrity Pact duly signed by the bidder shall be considered to be a non-responsive bid and shall be re-**

jected straightway. This is a binding agreement between the Buyer and Bidders for specific contracts in which the Buyer promises that it will not accept bribes during the procurement process and Bidders promise that they will not offer bribes. Under this Pact, the Bidders for specific services or contracts agree with the Buyer to carry out the procurement in a specified manner. The Pre-Integrity Pact will be as per Format enclosed.

5.15.1 A Pre-Contract Integrity Pact shall be signed between the Buyer and the ISP. This is a binding agreement between the Buyer and Bidder in which both agree to enter into a Pre-Contract agreement to avoid all forms of corruption by following a system that is fair, transparent, and free from any influence prior to, during and subsequent to the currency of the Contract.

5.15.2 The ISP shall submit duly signed Pre-Contract Integrity Pact in original, strictly as per the format (without any deviation) enclosed with the T.E/RFP.

5.15.3 The Pre-Contract Integrity Pact shall be valid, from the effective date of the Contract, for a period extending up to 5 years or completion of contractual obligations whichever is later.

5.15.3.1 The Buyer has nominated the following as Independent Monitor (IEM) for this Pact.

1	Shri Rajendra Kalla, CES, Ex-ADG/CPWD (Retd).	16 Munirka Enclave, Opp. Vasant Vihar Bus Depot, New Delhi-110067. Email ID: rajendra432000@yahoo.co.in

Any change/addition/deletion in the details of IEM will *ipso facto* result into the corresponding change of these details in the Integrity Pact.

6. SECTION V: SPECIAL CONDITIONS OF RFP

6.1 Performance Guarantee:

a. Successful bidder will be required to submit performance security within 30 days of effective date contract for due performance of contract. The amount of performance security will be 5% of contract value in Indian Rupees or Foreign Currency stipulated in contract, in Favour of "CMD, MUNITIONS INDIA LIMITED". Performance Bank Guarantee shall be issued from commercial bank and shall be valid for up to 60 days beyond the date of Contract expiry/Contract Termination in the enclosed format. Performance Security will be forfeited and en-cashed by the Buyer in the event of breach of contract by the ISP/Seller.

b. PSD may be submitted in the form of Account Payee Demand Draft (DD), Fixed Deposit Receipt (FDR), Banker's Cheque or Bank Guarantee (BG) on non-judicial stamp paper in specified format, safeguarding the purchaser's interest in all respects. Because of limited validity period of demand draft and banker's cheque, they shall be deposited in the MIL account and the same amount will be refunded to bidders, as applicable.

c. Failure to submit performance security may entail cancellation of contract

d. In case any claims or any other contract obligations are outstanding, the Seller will extend the Performance Bank Guarantee as asked for by the Buyer till such time as the ISP / Seller settles all claims and completes all contract obligations. The Performance Bank Guarantee will be subject to encashment by the Buyer, in case the conditions regarding adherence to delivery schedule, settlement of claims and other provisions of the contract are not fulfilled by the ISP / Seller. The format of PBG is enclosed.

6.2 Payment Terms:

It will be mandatory for the Bidder to indicate their Bank account numbers, GST details and other relevant e-payment details so that payments could be made through ECS/NEFT/RTGS mechanism. The payment will be made as per the following terms, on producing of the required documents: Payment will be guided differently for different components of the Contract, as below.

Sr. No.	Item	Description	Payment
1	Service Charges per Quarter	Service Charges per Quarter for IaaS based platform for DC/DR Services	As per Quarterly Invoice less applicable Penalties

All payments will normally be made by MIL within 30 days from the date of receipt of invoice along with supporting document like

(a) Commercial tax Invoice

(b) Proof of submission of PSD.

(c) Job Completion report from the authorised signatory of user (MIL)
(d) Performance report of the quarter (If applicable)
(e) Penalty calculation (if any)

6.3 **Advance Payments:**
No advance payment(s) will be made.

6.4 **Force Majeure Clause & Events of Default:**

6.4.1 **Force Majeure:**

6.4.1.1 Neither party shall bear responsibility for the complete or partial non-performance of any of its obligations (except for failure to pay any sum which has become due on account of receipt of goods under the provisions of the present Contract), if the non-performance results from such Force Majeure circumstances as Flood, Fire, Earth Quake and other acts of God as well as War, Military operation, blockade, Acts or Actions of State Authorities or any other circumstances beyond the party's control that have arisen after the conclusion of the present Contract.

6.4.1.2 In such circumstances the time stipulated for the performance of an obligation under the present Contract is extended correspondingly for the period of time of action of these circumstances and their consequences.

6.4.1.3 The party for which it becomes impossible to meet obligations under this Contract due to Force Majeure conditions, is to notify in written form the other party of the beginning and cessation of the above circumstances immediately, but in any case, not later than 10 (Ten) days from the moment of their beginning.

6.4.1.4 A certificate from a Chamber of Commerce (Commerce and Industry) or other competent authority or organization of the respective country shall be sufficient proof of commencement and cessation of the above circumstances.

6.4.1.5 If the impossibility of complete or partial performance of an obligation lasts for more than 6 months, either party hereto reserves the right to terminate the Contract totally or partially upon giving prior written notice of 30 (thirty) days to the other party of the intention to terminate without any liability other than reimbursement on the terms provided in the agreement for the goods received.

6.4.2 **Events of Default – ISP:**

"ISP Event of Default" means any of the following events unless such an event has occurred as a consequence of a Force Majeure Event: -

6.4.2.1 ISP's failure to perform or discharge any of its obligations in accordance with the provisions of this Contract.

6.4.2.2 The services in accordance with the provisions of given Contract are not available for more than 7 (Seven) continuous days during Contract period.

6.4.2.3 Any representation made or warranties given by ISP under a given Contract is found to be false or misleading.

6.4.2.4 Breach of any clause or part thereof of the "Integrity Pact" signed by the Parties pursuant to the RFP.

6.4.2.5 Appointment of a provisional liquidator, administrator, trustee or receiver of the whole or substantially whole of the undertaking of ISP by a court of competent jurisdiction in proceedings for winding up or any other legal proceedings.

6.4.2.6 The Performance Bank Guarantee and any other securities required to be maintained in the given Contract are not maintained in terms of the provisions hereof.

6.4.2.7 ISP abandons or expresses its intention to revoke/terminate as per given Contract without being entitled to do so as is expressly provided in the Contract.

6.4.2.8 Amalgamation of ISP with any other company or reconstruction or transfer of the whole or part of the Contract or the revenue earning parts of the Contract.

6.4.2.9 ISP engages or knowingly allows any of its employees, agents, Contractor or representative to engage in any activity prohibited under this Contract and/or by law or which constitutes a breach of the Contract or breach of or an offense under any law, in the course of any activity undertaken pursuant to this Contract.

6.4.2.10 Any Breach of Cyber security / Theft of Data/ Information by ISP or his representative.

6.5 Guarantee Clause:

The supplier shall guarantee satisfaction of technical and other parameters mentioned in the specification and Contract.

6.6 Non-Disclosure Agreement:

A Non-Disclosure Agreement will have to be signed by the Bidder. The format for Non-Disclosure Agreement is given in Form 9 of Annexure -A and will be signed with the Contract prior to start of their work confirming that there will be no disclosure of any information regarding hardware, software, configuration, password or any other information regarding MIL. Bidder will have to abide by the Non-Disclosure Agreement even after the completion of the Contract.

6.7 Third Party Contracts:

6.7.1 The Contracts executed by ISP to procure any of the services to be used by ISP for MIL DC/DR setup, including but not limited to development tools, testing facilities, outsourcing Contracts are to be treated as third party Contracts.

6.7.2 The third-party Contracts are owned by ISP and the liability for these Contracts lies solely with ISP.

6.7.3 In the event of termination of the Contract, ISP shall transfer/assign or cause to be transferred/assigned to the BUYER or its nominee such third-party Contracts which are valid and which the BUYER has chosen to take over at its sole discretion as per Exit Management Process.

6.8 Exit Management:

6.8.1 Initiation

6.8.1.1 This schedule sets out the provisions, which will apply on expiry or termination of the Contract.

6.8.1.2 In case of expiry of the Contract the provisions of this schedule come into effect three months before the Contract comes to an end.

6.8.1.3 However, if the BUYER, in the intervening period, invokes the provisions of the Contract and extends the term of the Contract, the provisions of the schedule will not come into effect.

6.8.2 Exit Management Plan

Exit management refers to the process of managing the removal or transition of ISP in case of events of default/ some exceptional cases.

6.8.2.1 On the initiation of the provisions of the exit management by the BUYER, ISP shall provide the BUYER with a recommended exit management plan which shall deal with at least the following aspects of exit management in relation to the Contract. Such exit management plan shall be arrived at with mutual consent.

6.8.2.2 A detailed program of the transfer process that could be used in conjunction with a replacement ISP including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.

6.8.2.3 Plans for the communication with replacement ISP and replacement ISP's sub-Contractors, staff, suppliers, and any related third party as are necessary to avoid any material detrimental impact on DC/DR services as a result of undertaking the termination or expiry.

6.8.2.4 The proposed arrangements for the segregation of communication means (including but not limited to transfer of data in electronic forms, email etc.) from the Networks employed by the BUYER and identification of specific security tasks necessary for ensuring this.

6.8.2.5 Plans for provision of contingent support to the BUYER and replacement ISP for a reasonable period after transfer.

6.8.2.6 The plan for settling the payments and claims pursuant to the Contract, if applicable.

6.8.2.7 The acceptance mechanisms for successful completion of exit management.

6.8.2.8 Payments during the Exit Management period shall be made in accordance with the mutually agreed Exit management plan.

6.8.2.9 This Exit Management plan shall be furnished in writing to the BUYER within 7 days of the date on which the action for termination is initiated or ninety days prior to the date of expiry of the Contract.

6.8.3 **Confidential Information, Security and Data:**

ISP will promptly on the commencement of the exit management period, hand over to the BUYER the following: -

6.8.3.1 Information relating to the current services rendered.

6.8.3.2 It is re-iterated that the data at DC/DR servers belongs to the BUYER and is Confidential Information.

6.8.3.3 Documentation relating to subcontractors.

6.8.3.4 All current and updated data of the DC/DR, transitioning the services to its replacement ISP will be provided in a mutually accepted process.

6.8.3.5 All other information (including, but not limited to, documents, records and Contracts) relating to the services reasonably necessary to enable the BUYER or its nominated agencies, or its replacement ISP to carry out due diligence in order to transition the provision of the services to the BUYER or its nominated agencies, or its replacement ISP (as the case may be).

6.8.3.6 Before the expiry of the exit management period, ISP shall deliver to the BUYER; all new or up-dated materials and shall not retain any copies thereof.

6.8.4 **Knowledge Transfer:**

6.8.4.1 ISP will undertake the following activities to ensure that the knowledge about the, Data Center, Disaster Recovery Center and the Networks, are transferred to the Buyer Team or the Replacement ISP. The activities will be aimed at:

(a) Knowledge transfer of operations.

(b) Knowledge transfer of technology.

(c) Knowledge transfer of processes.

6.8.4.2 Some of the key activities to be carried out by ISP for knowledge transfer will be:

(a) Joint operations of key activities or services of help desk, Data Center and DR Center operations.

(b) Briefing sessions on process and process documentation.

(c) Walk through the logs.

6.8.4.3 Transfer technology and up-to-date know-how relating to operation and maintenance of the DC/DR setup.

6.8.5 **General Obligations of ISP:**

6.8.5.1 ISP will involve the services of the subcontractors or the OEMs as the case may be, for the purpose of executing the exit management plans, without any costs to the BUYER.

6.8.5.2 ISP shall provide all information as mentioned in the above clauses in order to affect as seamless handover as practicable in the circumstances.

6.8.5.3 For the purposes of this Schedule, anything in the possession or control of ISP, any associated entity, or sub-contractor is deemed to be in the possession or control of ISP.

6.8.5.4 ISP shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

6.8.5.5 The task of ISP with reference to the exit management is deemed to be complete only when the Project Director of the BUYER issues a satisfactory completion certificate for the "exit management plan".

6.8.6 **BUYER's Obligations on Termination:**

On termination of the Contract, the Buyer's obligations towards ISP will be as follows:

6.8.6.1 The BUYER confirms that the payment for the last invoice by ISP will be expedited subject to the set off rights.

6.9 **Declaration of GO LIVE:**

6.9.1 After completion of DC/DR setup, ISP will submit the notice of readiness for declaring "GO LIVE".

6.9.2 MIL will decide on the actions to be taken on "GO LIVE" along with their system integrator partner.

6.9.3 The GO LIVE date comes into effect only when the MIL approves the notice for GO LIVE and Go-Live is effected or after 30 days of notice of declaration whichever is earlier.

6.10 Information Security and Audit Rights:

6.10.1 Information Security

6.10.1.1 The ISP shall report forthwith in writing to MIL all identified attempts (whether successful or not) by unauthorized persons either to gain access to or interfere with the DC/DR Data, facilities or Confidential Information.

6.10.1.2 ISP shall participate in regular meetings when safety and Information Technology security matters are reviewed.

6.10.1.3 The ISP shall promptly report in writing to MIL any act or omission which they are aware could have an adverse effect on the proper conduct of safety and information technology security at the DC/DR.

6.10.1.4 The ISP acknowledge that a high level of security needs to be maintained. All persons employed by ISP for this Contract shall undergo verification as per regulations.

6.10.1.5 ISP undertakes to meet the laid down security requirements/stipulations as per the Contract. All the matters related to the Contract will be treated as classified and highly confidential and shall not be communicated to anybody (except for the purpose of this Contract) or published/advertised without the consent of the BUYER.

6.10.2 Confidential Information:

6.10.2.1 ISP recognizes that during the term of the Contract, sensitive data will not be made available to its sub-contractors and agents and others working for or under ISP without express written permission from MIL. Further, ISP also recognizes that any improper and unauthorized disclosure or usage of DC/DR data by any such recipient may constitute a breach of applicable laws causing harm not only to BUYER but also the stakeholders whose data is used. Any breach of any confidentiality obligation set out in the Contract will result in BUYER a right to seek injunctive relief and damages suffered or are reasonably likely to be suffered and the cost incurred to mitigate the implication of such disclosure or usage, from ISP.

6.10.2.2 "Confidential Information" means any and all information that is or has been received by ISP (the "Receiving Party") from MIL (the "Disclosing Party") or that: (a) relates to the Disclosing Party; and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.

6.10.2.3 "Confidential Materials" shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and server disks or tapes, whether machine or user readable.

6.10.3 **Managing Confidential Information:**

6.10.3.1 The Receiving Party agrees to regard, preserve and keep as confidential all confidential information and materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:

(a) Disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, Company or any other entity other than its directors, partners, advisers, agents or employees. The Receiving Party agrees to be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees is in accordance with the terms and conditions of this Contract; or

(b) Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers.

6.10.3.2 In maintaining confidentiality hereunder, the Receiving Party on receiving the Confidential Information and materials agrees and warrants that it shall:

(a) Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own Confidential Information of like importance and such degree of care shall be at least that which is reasonably calculated to prevent such inadvertent disclosure.

(b) Keep the Confidential Information and materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party.

(c) Upon discovery of any unauthorized disclosure of Confidential Information, promptly inform the MIL of such disclosure in writing and immediately return to the MIL all such Information and materials, in whatsoever form, including any and all copies thereof.

6.10.3.3 The restrictions in this Para shall not apply to:

(a) Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this Contract); or

(b) Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any

inquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure; or

6.10.3.4 The Receiving Party agrees that its obligation under this Section with respect to confidentiality will survive the termination of this Contract.

6.10.3.5 Confidential Information shall be and remain the property of the MIL and nothing in this Contract shall be construed to grant either Party any right or license with respect to the other Party's Confidential Information otherwise than as is expressly set out in this Contract.

6.10.3.6 ISP agrees that monetary damages would not be a sufficient remedy for any breach of this Contract by ISP and that the BUYER, as appropriate, shall be entitled to equitable relief, including injunction and specific performance as a remedy for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach by ISP of this Contract but shall be in addition to all other remedies available at law or equity to the damaged Party.

6.10.4 **Information Ownership:**

6.10.4.1 ISP understands and agrees that civil, criminal, or administrative implications may arise for failure to protect information appropriately.

6.10.4.2 ISP agrees that.

(a) All customers', suppliers', associated organizations and process related information of the BUYER is considered as sensitive and will be protected from unauthorized disclosure, modification or access.

(b) Any sensitive information of the BUYER would be protected from unauthorized disclosure, modification or access.

6.10.5 **Privacy and Security Safeguards:**

6.10.5.1 ISP agrees not to publish or disclose in any manner, under any circumstances the details of any security safeguards implemented by ISP under this Contract.

6.10.5.2 ISP agrees to develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all the BUYER information, data and sensitive application software.

6.11 **Audit, Access and Reporting:**

6.11.1 **Purpose:**

This details the audit, access and reporting rights of the BUYER and respective obligations of ISP under the Contract.

6.11.2 **Audit Notice and Timing:**

6.11.2.1 As soon as reasonably practicable after the Effective Date, ISP shall use its best endeavours to agree to a timetable for routine audits of DC/DR. Such a timetable may be reviewed in future if required. During the Term, the BUYER or its nominated agencies shall conduct routine audits in accordance with the agreed timetable and shall not be required to give ISP any further notice of carrying out such audits.

6.11.2.2 The BUYER may conduct non-timetabled (adhoc) audits at its own discretion if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by ISP, a security violation, or breach of confidentiality obligations by ISP, provided that the requirement for such an audit is notified in writing to ISP a reasonable period time prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based. If ISP considers that the non-timetabled audit was not appropriate, the matter shall be referred to the Independent Monitor as defined in Contract.

6.11.2.3 The frequency of audits shall be mutually decided between ISP and MIL, provided always that the BUYER or MIL shall endeavour to conduct such audits with the lowest levels of inconvenience and disturbance as practicable being caused to ISP.

6.11.2.4 The audit and access rights contained shall survive the termination or expiration of the Contract for a period of six (6) months.

6.11.3 **Access:**

ISP shall provide to the BUYER or its nominated agencies, or their authorized representatives access to employees, subcontractors, suppliers, third party facilities, including leased premises, Data Recovery Centers, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The BUYER or its nominated agencies during the audit shall have the right to copy and retain copies of any relevant records. ISP shall make effort to co-operate with them in effecting the Audit. The Buyer shall not have access to the proprietary data of, or relating to, any other customer of the Bidder, or a third party or the Bidder's cost, profit, discount, and pricing data, without the prior approval of ISP. This approval must be provided by the ISP to the Buyer if requested under clause 5.6 of this RFP. The audit shall not be permitted if it interferes with the Bidder's ability to perform the services in accordance with the service levels, unless the Buyer relieves the

Bidder from meeting the applicable service levels.

6.11.4 **Audit Rights:**

The BUYER shall have the right to audit and inspect documents, records, procedures and systems relating to the DC/DR, but only to the extent that they relate to these, as shall be reasonably necessary to verify:

6.11.4.1 The security, integrity and confidentiality of all the BUYER Data processed, held or conveyed by ISP on behalf of the BUYER or its nominated agencies and its Users and documentation related thereto.

6.11.4.2 That ISP has complied with the relevant technical standards, and has adequate internal controls in place; and

6.11.4.3 The compliance of ISP with any other obligation under the Contract.

6.11.4.4 ISP's internal cost records shall be excluded for the purpose of audit.

6.11.4.5 That the actual level of performance of the Services is the same as that specified in the "Service Level Agreement" mentioned in clause 4.5.

6.11.5 **Action and Review:**

6.11.5.1 Any change or amendment to the systems and procedures of ISP, or sub-Contractors, where applicable, arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.

6.11.5.2 Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to the authorized person as designated by MIL from time to time, who shall determine what action shall be taken in respect of such discrepancies in accordance with the terms of the Contract.

6.11.6 **Records and information:**

For the purposes of audit in accordance with this Schedule, ISP shall maintain true and accurate records in connection with the provision of the services and ISP shall handover all the relevant records and documents upon the termination or expiry of the Contract.

6.12 **Escalation Procedures:**

(a) Irrespective of the nature of disputes, events, and defaults, the notices for discussion or resolution will follow the escalation procedures.

(b) The initiation of the escalation activities, other than the ones for termination, will be from the authorized representative of MIL or authorized representative of ISP.

(c) The escalations will follow the guidelines listed for each type of notices.

6.12.1 **Procedure for Issuing Notices:**

6.12.1.1 Subject to the provisions hereof, all notices hereunder shall be issued as per provision of Contract.

6.12.2.2 If the responding party fails to respond to the notice within 21 days of notice, a maximum of one more notice to the same effect may be issued to the party.

6.12.3.3 If the responding party does not respond to two notices, it is treated as wilful violation of the Contract, and the actions related to breach of Contract will come into force.

6.12.2 **Notices on Disputes:**

6.12.2.1 Either Party (“Claimant”) shall first submit any dispute or disagreement (dispute notice) is not a material breach of this Contract (a "Disputed Matter") to the <Designation of the person to whom it shall be reported>, with a copy to the other Party.

6.12.2.2 The dispute notices will be a written notice and shall be accompanied by:

(a) A statement by the Claimant describing the Disputed Matter in detail.

(b) Documentation, if any, supporting the Claimant's potion on the Disputed Matter.

6.12.2.3 The other Party ("Respondent") shall have the right to respond to the Dispute Notice within 7 days after receipt of the Dispute Notice.

6.12.2.4 The two designated authorities from both the parties will resolve the dispute through mutual discussion.

6.12.2.5 In case the Disputed Matter remains unresolved, the same shall then be submitted to higher management of both parties.

6.12.3 **Notice for Consultation:**

6.12.3.1 The Party shall submit a notice for consultation for an event of default to the Name of the person to whom it shall be reported, with a copy to the other Party,

6.12.3.2 The consultation notice will be accompanied by: -

(a) Description of the event of default.

(b) The date and circumstances of default.

(c) Documentary evidence if any of the event of default.

6.12.3.3 The other Party ("Respondent") shall have the right to respond to the Consultation Notice within 7 days after receipt of the Consultation Notice.

6.12.3.4 The respective authorities will initiate the remedial process, with specific action and time lines for action (not exceeding 90 days) to rectify the event of default, through mutual discussion.

6.12.4 **Notice of an Event:**

6.12.4.1 The Affected Party shall give notice on the event to the other Party of the occurrence of any event within 7 (seven) days after the Affected Party knew, or ought reasonably to have known, of its occurrence.

6.12.4.2 The Notice shall include details of: -

(a) The nature, time of occurrence and extent of the Force Majeure Event with documentary evidence in respect thereof.

(b) If the event is due to Change in Law, a certified copy of the changed law, the effective date of the law and a copy of the earlier law which was applicable when the Contract came into effect.

(c) If the event is due to Change in Law, the notice will also include the list of Contract or part of the Contract which will be impacted and suggestions if any for modification.

(d) Description of the adverse effect it has or is likely to have on the performance of the party's obligations under this Contract.

(e) The duration or estimated duration and the effect or probable effect the Event has or will have on the Affected Party's ability to perform its obligations or any of them under this Contract.

(f) The measures which the Affected Party has taken or proposes to take, to alleviate the impact of the Event or to mitigate the damage; and

(g) Any other relevant information.

6.12.4.3 If the notice of an event is accepted by the other Party as valid, the two Principal Officers will initiate the actions required to be undertaken and the periodicity (at least once in a month) for the affected party to submit reports on the event to the other party.

6.12.5 **Notices on Dispute Resolution and Termination:**

6.12.5.1 Notice for Dispute Resolution or termination will be issued when all the other mechanisms of dispute resolution listed in the consultation procedure as in clause 6.12.3 have failed to resolve or overcome the event.

6.12.5.2 The Dispute Resolution and termination notices will include:

(a) The details of events, default or disputes leading to arbitration or termination.

(b) In case of termination, a deadline and a plan of action for exit management.

6.13 **Indemnities, Limitation of Liabilities:**

6.13.1 **Third party Claims:**

6.13.1.1 ISP undertakes to indemnify the BUYER from and against all losses, claims or damages on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the BUYER) attributable to ISP's performance under this Contract.

6.13.1.2 The indemnities set out in this Contract shall be subject to the following conditions: -

(a) The BUYER, as promptly as practicable, informs ISP in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise.

(b) The BUYER may at its option (but shall not be obligated to), at the cost of ISP, give ISP assistance in the defence of such claim including access to all relevant information, documentation and personnel provided that the BUYER may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such defence.

(c) If ISP does not assume full control over the defence of a claim as provided in this Contract, the BUYER may participate in such defence at cost and expense of ISP.

(d) The BUYER shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of ISP.

(e) All settlements of claims subject to indemnification under this Contract will:

(i) Be entered into only with the consent of the BUYER, which consent will not be unreasonably withheld and include an unconditional release to the BUYER from the claimant for all liability in respect of such claim; and

(ii) Include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement.

(f) The BUYER shall account to ISP for all awards, settlements, damages and costs (if any) finally awarded in favour of the BUYER which are to be paid to it, in connection with any such claims or proceedings.

6.13.2 **Limitation of Liability:**

6.13.2.1 ISP's aggregate liability for actual direct damages shall be capped at [10%] of the Total Contract Value provided that this limit shall not apply to

(a) The bodily injury (including death) and damage to real property and tangible personal property caused by ISP's negligence and/or

(b) The intellectual property infringement claims.

6.13.2.2 ISP shall not in any event be liable for any indirect or consequential damages, or for loss of profit, business, revenue, goodwill, anticipated savings or Data, or third- party claims except with respect to bodily injury (including death) and damage to real and tangible personal property.

6.13.2.3 Neither this Contract nor the services delivered by ISP under this Contract grants or creates any rights, benefits, claims, obligations or causes of action in, to or on behalf of any person or entity (including any third party) other than between the respective Parties to this Contract, as the case may be.

6.13.2.4 Title and Risk of Loss: ISP shall bear the risk of loss on DC/DR setup. ISP shall arrange and pay for insurance to cover such an item.

6.14. **Independent Relationship:**

Nothing in this proposal shall be deemed to constitute a partnership, joint venture, agency or any kind of relationship between the parties or constitute any party as the agent of any other party for any purpose or entitle any party to commit or bind any other party in any manner or give

rise to fiduciary duties by one party in favor of any other.

6.15. **Entire understanding:**

This Proposal together with the Schedules, Annexure and Exhibits here to and executed by the party here to constitutes the entire understanding between the party here to with respect to the subject matter here to and supersedes and cancels all previous negotiations thereof.

6.16. **Survival:**

The clauses of this proposal which by their nature are intended to survive shall so survive the termination/expiry of this proposal.

6.17. **Publicity:**

ISP shall not publicize any information pertaining to this Contract without seeking the prior written consent of the other party.

6.18. **Modification:**

This proposal may be modified only by an amendment executed in writing by a duly authorized representative for each party.

6.19. **Waiver:**

No forbearance, indulgence or relaxation by any Party at any time to require performance of any provision of this Proposal shall in any way affect, diminish or prejudice the right of such party to require performance of that provision and any waiver by any party or any breach of any provisions of this Proposal shall not be construed as a waiver or an amendment of the provisions itself, or a waiver of any right under or arising out of this Proposal.

6.20. **Assignment:**

Buyer shall be entitled to assign or transfer all or any of its rights, benefits and obligations under this proposal without the prior written consent of the other Party.

7. SECTION VI: ANNEXURES

7.1 Annexure – A: Server Hardware Sizing:

(a) Hardware Sizing for DC Non-Production System:

Hardware Sizing for DC Non- Production System-Munitions India Limited								
Sr. No.	**System Type**	**Layer**	**Database**	**Operating System**	**Recommended SAPS at 65% CPU**	**Memory in GB**	**Internal Storage in GB**	**Storage in GB**
Development Landscape								
1	S/4 HANA DB	Database	SAP HANA Database	Linux		384	200	2304
2	S/4 HANA APPS	Application		Linux	16500	64	200	300
3	SAP BI-BO (Business Intelligence BusinessObjects)	Database + Application	Sybase	Linux	6000	32	200	512
4	SAP PO (Process Orchestration)	Database + Application	Sybase	Linux	Its Core based	4 Core / 24 GBRAM	200	512
5	Access Management	Database + Application	Sybase	Linux	6000	24	200	768
6	SAP MDM (Master Data Management)	Database + Application	Sybase	Linux	6000	24	200	512
7	BW4 / HANA + BPC DB	Database	HANA Database	Linux		256	200	2048
8	BW4 / HANA + BPC APPS	Application		Linux	6000	32	200	300
Quality Assurance Landscape								
9	S/4 HANA DB	Database	SAP HANA Database	Linux		768	200	4096
10	S/4 HANA Application server	Application		Linux	32500	128	200	300
11	SAP BI-BO (Business Intelligence Business Objects)	Database + Application	Sybase	Linux	12000	32	200	512
12	SAP PO (Process Orchestration)	Database + Application	Sybase	Linux	Its Core based	4 Core / 24 GB RAM	200	512
12.1	SAP PO (Process Orchestration)	Database + Application	Sybase	Linux	Its Core based	4 Core / 24 GB RAM	200	512
13	Access Management	Database + Application	Sybase	Linux	9000	24	200	768
14	SAP MDM (Master Data Management)	Database + Application	Sybase	Linux	9000	24	200	512
15	BW4 / HANA + BPC DB	Database	HANA Database	Linux		288	200	1728
16	BW4 / HANA + BPC APPS	Application		Linux	12000	64	200	300
Training Landscape								
17	S/4 HANA DB	Database	SAP HANA Database	Linux		768	200	4096
18	S/4 HANA Application server	Application		Linux	32500	128	200	300

Additional Component - Web Dispatcher								
19	Web Dispatcher - Development	Application		Linux	2000	16	200	100
20	Web Dispatcher - Quality	Application		Linux	2000	16	200	100

(b) Hardware Sizing for DC Production System:

Hardware Sizing for DC Production System-Munitions India Limited										
Sr.No.	**System Type**	**Layer**	**Data-base**	**Oper-ating System**	**Base SAPS at 65% CPU**	**Addi-tional Loading on Base SAPS**	**Recom-mended SAPS at 65% CPU**	**Memory in GB**	**Inter-nal Stor-age in GB**	**Stor-age in GB**
Production Landscape										
1	S/4 HANA - Primary	Database	SAP HANA Database	Linux				768	200	4096
2	S/4 HANA - Secondary (Fail-Over)	Database	SAP HANA Database	Linux				768	200	4096
3	S/4 HANA - HA (ASCS +PAS)	Applica-tion	SAP App server	Linux	34255	35%	46245	128	200	400
4	S/4 HANA - HA (ERS +Additional App server 1	Applica-tion	SAP App server	Linux	34255		46245	128	200	400
5	S/4 HANA - Additional App server2	Applica-tion	SAP App server	Linux	34255		46245	128	200	400
6	S/4 HANA - Additional App server3	Applica-tion	SAP App server	Linux	34255		46245	128	200	400
7	SAP BI-BO (Business Intelli-gence BusinessObjects)	Database + Applica-tion	SAP ASE Database	Linux			24249	64	200	1024
8	SAP PO (Process Orchestration)	Database + Applica-tion	SAP ASE Database	Linux			Its Core based	4 Core / 64 GB RAM	200	512
8.1	SAP PO (Process Orchestration)	Database + Applica-tion	SAP ASE Database	Linux			Its Core based	4 Core / 64 GB RAM	200	512
9	Access Management	Database + Applica-tion	SAP ASE Database	Linux	10721	20%	12865	48	200	768
10	Solution Manager DB	Database	SAP HANA DB	Linux				256 GB	200	1536
11	Solution Manager (ABAP and JAVA Stack) + SAPROUTER	Applica-tion & SAP Router	Application	Linux			14000	96	200	400
12	SAP MDM (Master Data Man-agement)	Database + Applica-tion	SAP ASE Database	Linux	12000	20%	14400	48	200	512
13	BW4 / HANA + BPC DB	Database	SAP HANA Database	Linux				288	200	1728
14	BW4 / HANA + BPC APPS	Applica-tion 1	SAP App server	Linux	8691	35%	11733	64	200	400
15	BW4 / HANA + BPC APPS	Applica-tion 2	SAP App server	Linux	8691		11733	64	200	400

Additional Component - Web Dispatcher										
16	Web Dispatcher - Production	Applica-tion	SAP Appli-cation	Linux			2000	16	200	100

(c) Hardware Sizing for DR Production System:

Hardware Sizing for DR Production System-Munitions India Limited										
Sr.No.	**System Type**	**Layer**	**Data-base**	**Oper-ating System**	**Base SAPS at 65% CPU**	**Addi-tional Loading on Base SAPS**	**Recom-mended SAPS at 65% CPU**	**Memory in GB**	**Inter-nal Stor-age in GB**	**Stor-age in GB**
Production Landscape										
1	S/4 HANA - DR	Database	SAP HANA Da-tabase	Linux				768	200	4096
2	S/4 HANA - DR	Application - DR		Linux			46245	128	200	400

(d) HANA DB Memory Sizing:

HANA Database Memory Sizing- Munitions India Limited (In GB)				
Sr. No.	**Component's**	**Year 1**	**Year 2***	**Year 3***
1	S/4 HANA Development	256	320	384
2	S/4 HANA Quality	384	576	768
3	S/4 HANA Production	384	576	768
4	S/4 HANA Production HA	384	576	768
5	S/4 HANA Production DR	384	576	768

* Are indicative for future expansion

(e) Additional Storage Sizing for Other Solution:

Sr. No.	System Type	Database	Operating Sys-tem	Memory in GB	Internal Storage in GB	Storage in GB
1	DMS Server (Non-Produc-tion): DC		Windows/Linux	4 Core / 32 GB	200 GB	500 GB
2	DMS Server (Production): DC		Windows/Linux	8 Core / 64 GB	200 GB	1 TB
3	DMS Server (Production): DR		Windows/Linux	8 Core / 64 GB	200 GB	1 TB
4	Anti-Virus Server: DC for DMZ		Windows/Linux	64 GB	250 GB	250 GB
5	Anti-Virus Server: DC for ComNet		Windows/Linux	64 GB	250 GB	250 GB

6	Planvisage Server: DC	MS SQL Ser	Windows/Linux	4 Core /128 GB	200 GB	1 TB
7	Planvisage Server: DR	MS SQL Ser	Windows/Linux	4 Core /128 GB	200 GB	1 TB
8	Patch Management Server: DC		Windows/Linux	64 GB	250 GB	250 GB
9	PHP Web Server (For Non-ERP Server): DC for ComNet	MySQL/In-formix	Windows/Linux	128 GB	250 GB	512 GB
10	PHP Web Server (For Non-ERP Server): DC for DMZ	MySQL/In-formix	Windows/Linux	128 GB	250 GB	512 GB
11	PHP Web Server (For Non-ERP Server): DR for ComNet	MySQL/In-formix	Windows/Linux	128 GB	250 GB	512 GB
12	MySQL/Informix Server): DC for ComNet		Windows/Linux	128 GB	250 GB	1 TB
13	MySQL/Informix Server: DC for DMZ		Windows/Linux	128 GB	250 GB	1 TB
14	ITSM Server: DC		Windows	8 Core/ 64 GB	480 GB	2048 GB

Storage Sizing for Other Solutions - Munitions India Limited (In GB)				
Sr. No.	**Component's**	**Year 1**	**Year 2***	**Year 3***
1	DMS Database	500 GB	1 TB	1.5 TB
2	MS SQL Server (Planvisage)	1 TB	1.5 TB	2 TB
3	MySQL Server/Informix	1 TB	1.5 TB	2 TB
4	ITSM	2 TB	2.5 TB	3 TB

* Are indicative for future expansion

The following Servers to be installed in DMZ Zone.

1. PO (Process Orchestration): 1 No. at DC
2. SAP Router: 1 No. at DC
3. Anti-Virus: 1 No. DC
4. PHP: 1 No. at DC
5. MySQL: 1 No. at DC

The ISP shall prepare Standard Operating Procedure (SOP) which will be mutually agreed by ISP and MIL for the Operation of the Servers to be installed in DMZ zone to segregate Internet Environment from MIL Intranet at DC to achieve Air-Gap between Internet and MIL Intranet.

(f) Air-gap Technique:

Segregation of Internet Environment from MIL Intranet at DC/DR			
Sr. No.	**Server in DMZ Zone**	**Requirement**	**Process for Access**
1	PO (Process Orches-tration)	SAP's middleware software for enabling the interface capabilities to connect with third party systems. e.g., Banks, GEM and CPP etc. This helps segregating the main SAP S/4HANA and only SAP PO enables the token based / file-based information sharing.	Ports on External & Internal Firewall will be opened to carry out respective activities on the servers. Once activity is completed, Port will be shut down on both Firewalls to deny the access from Internet.
2	Anti-Virus	It is required for getting latest patches and signatures from OEM to enable patch up-dates and update signature on servers at DC/DR.	
3	PHP	This system will be Quality system for testing and audit of MIL Web applica-tions which are hosted on the MIL web portal on NIC servers.	
4	MySQL	This database server will be supporting the quality system on the PHP servers.	

7.2 Annexure – B: Forms for General Bidding Process:

7.2.1 Form 1: Format for List of Hardware/Software

<< Company Letter Head >>

LIST OF HARDWARE/SOFTWARE

[Date]

To

Munitions India Limited
Corporate Office: 2nd Floor Nyati Unitree
Nagar Road, Yerwada Pune – 411006
Contact: 020-67080400
mil-pune@munitionsindia.in
Sir,

Sub: List of Hardware/Software Components required at DC/DR for ERP Solution for MIL

The Bidder is requested to provide the list of Hardware/Software components to be installed at DC & DR setups as per the proposal along with technical specification of each item.

-

-

The Bidder can provide this information in their own format.

Yours faithfully,

Authorized Signatory

Designation

Company Seal

7.2.2 **Form 2: Format for Conflict of Interest:**

<< Company Letter Head >>

CONFLICT OF INTEREST

[Date]

To

Munitions India Limited
Corporate Office: 2nd Floor Nyati Unitree
Nagar Road, Yerwada Pune – 411006
Contact: 020-67080400
mil-pune@munitionsindia.in
Sir,

Sub: Undertaking on Conflict of Interest regarding Implementation of DC/DR for ERP Solution at MIL

I/We do hereby undertake that there is absence of actual or potential conflict of interest on the part of the Bidder or any prospective subcontractor due to prior, current, or proposed Contracts, engagements, or affiliations with MIL.

I/We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact our ability to complete the requirements as given in the RFP.

We undertake and agree to indemnify and hold MIL harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisers (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees and fees of professionals, reasonably) by MIL and/or its representatives, if any such conflict arises later.

Yours faithfully,

Authorized Signatory

Designation

Company Seal

7.2.3 **Form 3: <u>Format for Performance Bank Guarantee:</u>**

<u>PERFORMANCE BANK GUARANTEE</u>

From
Bank: ……

To,
The CMD,
Munitions India Limited,
Corporate Office: 2nd Floor Nyati Unitree,
Nagar Road, Yerwada, Pune – 411006
Contact: 020-67080400
<u>mil-pune@munitionsindia.in</u>

Dear Sir,

1 Whereas you (the "PURCHASER") have entered into a contract No…….. dated (hereinafter referred to as the "said Contract") with M/s ……..(hereinafter referred to as the "SELLER") for supply of goods as defined in the said Contract and whereas the SELLER has undertaken to produce a bank guarantee for ……% of total contract value amounting to …….. (amount of the guarantee in figures and words) to secure its obligations to the PURCHASER in accordance with the said Contract.

2 We……..(the Bank) hereby expressly, irrevocably and unreservedly undertake and guarantee as principal guarantor on behalf of the SELLER that, we will pay you on your demand declaring the SELLER to be in default under the said Contract, without demur or contest, all and any sum up to a maximum of Rupees…….. only. Your written demand shall be conclusive evidence to us that such repayment is due under the terms of the said Contract.

3 We undertake to effect payment upon receipt of such written demand, notwithstanding any dispute or disputes raised by the SELLER in any suit pending before any Court, Tribunal, Arbitrator or any other authority, our liability under this present being absolute and unequivocal.

4 We shall not be discharged or released from this undertaking and guarantee by any arrangements or variations made between you and the SELLER, indulgence to the SELLER by you or by any alterations in the obligation of the SELLER or by any forbearance whether as to payment, time, performance or otherwise.

5 In no case shall the amount of this guarantee be increased.

6 This guarantee shall remain in full force and effect until two months beyond the warranty period as specified in the contract i.e. up to _____ (expiry date) *[^or*

until the PURCHASER has signed the Final Acceptance Certificate (FAC) and has received the contractually agreed Warranty Bond as per the said Contract]. In case of delay in fulfilment of obligations by the SELLER, the expiry date shall be extended by us as per intimation from the SELLER.

7 Unless a demand or claim under this guarantee is made to us in writing on or before the aforesaid expiry date or extended expiry date, all your rights under this guarantee shall be forfeited and we shall be discharged from the liabilities hereunder.

8 This guarantee shall be continuing guarantee and shall not be discharged by any change in the constitution of the Bank or in the constitution of the SELLER.

9 We lastly undertake not to revoke this guarantee during its currency except with the previous consent of the PURCHASER in writing.

Yours faithfully,
For _____ Bank
(Authorised Signatory)
Seal of the Bank

Place :

Date :

7.2.4 **Form 4: Format for Pre-Contract Integrity Pact:**

PRE-CONTRACT INTEGRITY PACT

(For cases valuing above Rs. 5 Cr)

Ref: Tender Enquiry No ……..…. Dated …….

General

1. Whereas the CGM, hereinafter referred to as the Buyer and the first party, proposes to procure (Name of the Store/ Equipment), hereinafter referred to as Defence Stores, and M/s _____,represented by, Mr/ Mrs_____, Chief Executive Officer(which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignees), hereinafter referred to as the Bidder/Seller and the second party, is willing to offer/has offered the stores.

2. Whereas the Bidder is a private company/public company/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the Buyer is Munitions India Limited (MIL) or any of its constituent units, a PSU under Ministry of Defence, Government of India.

Objectives

3. Now, therefore, the Buyer and the Bidder agree to enter into this pre-contract agreement, hereinafter referred to as payment, to avoid all forms of corruption by following a system that is fair, transparent and free from any influence / unprejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

3.1 Enabling the Buyer to obtain the desired defence stores at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

3.2 Enabling bidders to abstain from bribing or any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also refrain from bribing and other corrupt practices and the Buyer will commit to prevent corruption, in any form, by their officials by following transparent procedures.

Commitments of the Buyer

4. The Buyer Commits itself to the following:-

4.1 The Buyer undertakes that no official of the Buyer, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Bidder, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the Contract.

4.2 The Buyer will, during the pre-contract stage, treat all Bidders alike, and will provide to all Bidders the same information and will not provide any such information to any particular Bidder which could afford an advantage to that particular Bidder in comparison to other Bidders.

4.3 All the officials of the Buyer will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

5. In case of any such preceding misconduct on the part of such official(s) is reported by the Bidder to the Buyer with full and verifiable facts and the same is prima facie found to be correct by the Buyer, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the Buyer and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the Buyer the proceedings under the contract would not be stalled.

Commitments of Bidders

6. The Bidder commits himself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of his bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commits himself to the following:-

6.1 The Bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Buyer, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the Contract.

6.2 The Bidder further undertakes that he has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Buyer or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the Contract or any other Contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the Contractor any other Contract with the Government.

6.3 The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

6.4 The Bidder will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

6.5 The Bidder further confirms and declares to the Buyer that the Bidder is the original manufacturer/integrator/ authorised government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the Buyer or any of its functionaries, whether officially or unofficially to the award of the contract to the Bidder, nor has any amount been paid, promised or

intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

6.6 The Bidder, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the Buyer or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

6.7 The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The Bidder also undertakes to exercise due and adequate care lest any such information is divulged.

6.8 The Bidder commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

6.9 The Bidder shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

7. **Previous Transgression**

7.1 The Bidder declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India, that could justify bidder's exclusion from the tender process.

7.2 If the Bidder makes incorrect statement on this subject, Bidder can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

8. **Earnest Money/Security Deposit**

8.1. **All procurement cases above Rs. 5 Cr., Integrity Pact is required to be executed without any additional Financial Guarantee**. The EMD/SD/PBG required to be submitted by the vendor as prescribed in the respective Procurement Manual shall only act as the financial guarantee for the IP.

8.2. The validity of the IP will be the validity of the EMD/SD/PBG or the complete conclusion of contractual obligations to complete satisfaction of both the bidder and the buyer, whichever is later. In case there are more than one bidder, the Earnest Money/Security Deposit shall be refunded by the buyer to those bidder(s) whose bid does not qualify (do not qualify) after the stages of TEC/ TPC, as constituted by the Buyer, immediately after a recommendation is made by the TEC/TPC on bid(s) after an evaluation.

8.3 In the case of successful bidder a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the Buyer to forfeit the same without assigning any reason for imposing sanction for violation of this pact.

8.4 The provisions regarding Sanctions for Violation in Integrity Pact include forfeiture of Performance Bond in case of a decision by the Buyer to forfeit the same without assigning any reason for imposing sanction for violation of Integrity Pact.

8.5 No interest shall be payable by the Buyer to the Bidder(s) on Earnest Money/Security Deposit for the period of its currency.

9. **Company Code of Conduct**

9.1 Bidders are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behaviour) and a compliance program for the implementation of the code of conduct throughout the company.

10. **Sanctions for Violation**

10.1 Any breach of the aforesaid provisions by the Bidder or any one employed by him or acting on his behalf (whether with or without the knowledge of the Bidder) or the commission of any offence by the Bidder or any one employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act 1988 or any other act enacted for the prevention of corruption shall entitle the Buyer to take all or any one of the following actions, wherever required:-

(i) To immediately call off the pre-contract negotiations without assigning any reason or giving any compensation to the Bidder. However, the proceedings with the other Bidder(s) would continue.

(ii) The Earnest Money/Security Deposit/Performance Bond shall stand forfeited either fully or partially, as decided by the Buyer and the Buyer shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the Bidder.

(iv) To recover all sums already paid by the Buyer, and in case of an Indian Bidder with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India (or Base Rate of State Bank of India in the absence of Prime Lending Rate) and in case of a Bidder from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the Bidder from the Buyer in connection with any other contract for any other defence stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance-cum-warranty bond, if furnished by the Bidder, in order to recover the payments, already made by the Buyer, along with interest.

(vi) To cancel all or any other Contracts with the Bidder.

(vii) To ban the Bidder from entering into any bid from the Government of India for a minimum period of five years and not more than ten years at the discretion of the Buyer.

(viii) To recover all sums paid in violation of this Pact by Bidder(s) to any middleman or agent or broker with a view to securing the contract.

(ix) If the Bidder or any employee of the Bidder or any person acting on behalf of the Bidder, either directly or indirectly, is closely related to any of the officers of the Buyer, or alternatively, if any close relative of an officer of the Buyer has financial interest/stake in the Bidder‟s firm, the same shall be disclosed by the Bidder at the time of filing of tender. Any failure to disclose the interest involved shall entitle the Buyer to rescind the contract without payment of any compensation to the Bidder.
The term „close relative‟ for this purpose would mean spouse whether residing with the Government servant or not, but not include a spouse separated from the Government servant by a decree or order of a competent court; son or daughter or step son or step daughter and wholly dependent upon Government servant, but does not include a child or step child who is no longer in any way dependent upon the Government servant or of whose custody the Government servant has been deprived of by or under any law; any other person related, whether by blood or marriage, to the Government servant or to the Government servant‟s wife or husband and wholly dependent upon Government servant.

(x) The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the Buyer, and if he does so, the Buyer shall be entitled forthwith to rescind the contract and all other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to the Buyer resulting from such rescission and the Buyer shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

(xi) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the Buyer with the Bidder, the same shall not be opened.

10.2 The decision of the Buyer to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder shall be final and binding on the Bidder, however, the Bidder can approach the monitor(s) appointed for the purposes of this Pact.

11. **Fall Clause**

11.1 The Bidder undertakes that he has not supplied/is not supplying the similar systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India and if it is found at any stage that the similar system or sub-system was supplied by the Bidder to any other Ministry/Department of the Government of India at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Buyer, if the contract has already been concluded.

11.2 The Bidder shall strive to accord the most favoured customer treatment to the Buyer in respect of all matters pertaining to the present case.

12. **Independent Monitors**

12.1 The Buyer has appointed Independent Monitor(s) for this Pact in consultation with the Central Vigilance Commission (**Names and Addresses of the Monitors to be given**):

12.2 As soon as the Monitor notices, or believes to notice, a violation of this Pact, he will so inform **the CGM.**

13. **Examination of Books of Accounts**
In case of any allegation of violation of any provisions of this Integrity Pact or payment of commission, the Buyer or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

14. **Law and Place of Jurisdiction**
This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the Buyer i.e. **the nearest location from the seat of the Buyer of a High Court or a Bench of High Court**.

15. **Other Legal Actions**
The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

16. **Validity**

16.1 The validity of this Integrity Pact shall be from date of its signing and will remain valid upto the validity of the PBG or the complete conclusion of contractual obligations to complete satisfaction of both the Buyer and the Bidder/Seller, whichever is later.
16.2 Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

17. The Parties hereby sign this Integrity Pact at _____ on _____

BUYER	**BIDDER**
( )	( )
Designation:	Chief Executive Officer
Ordnance Factory_____	Name of Firm:_____
Witness	**Witness**
1. _____	1. _____
2. _____	2. _____

7.2.5 Form 5: Format for Proposal Covering Letter

<< Company Letter Head >>

PROPOSAL COVERING LETTER

[Date]

To,

Munitions India Limited
Corporate Office: 2nd Floor Nyati Unitree
Nagar Road, Yerwada Pune – 411006
Contact: 020-67080400
mil-pune@munitionsindia.in

Ref: RFP for Implementation of DC/DR for the SAP S/4 HANA ERP Solution at MIL

Dear Sir,

This is to notify you that our company intends to submit a proposal in response to the RFP for implementation of the DC/DR for SAP S/4 HANA ERP solution at MIL.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to the MIL are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the MIL in its short-listing process.

The following persons will be the authorized representatives of the company for all the future correspondence till the completion of the bidding process, between MIL and our organization.

	Primary Contact	**Secondary Contact**
Name of the Person:		
Job Title:		
Name of the Company:		
Address:		
Phone:		
Mobile:		
Fax:		
E-mail:		

We understand that it will be the responsibility of our organization to keep MIL posted of any changes in this list of authorized persons and we fully understand that MIL shall not be responsible for non-receipt

or non-delivery of any communication and/or any missing communication in the event prior notice of any change in the authorized person(s) of the company is not provided to MIL.

We undertake that we will deploy only persons of Citizens of India in the execution of this Contract if awarded to us.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company/ firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of 2024

(Signature) (In the capacity of)

Duly authorized to sign the RFP Response for and on behalf of:

Sincerely,

[The Company's name]

Name

Title

Signature

Date

(Name and Address of Company) Seal/Stamp of the Company

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am ……<designation>…… of the ……<Company Name>……., and that ……<Name of the Respondent>…… who signed the above response is authorized to bind the corporation by authority of its governing body.

Date

(Seal here)

7.2.6 Form 6: Format for Checklist

<< Company Letter Head >>

CHECKLIST

Sr. No	Description	Format	Submitted
1	Form 1	List of Hardware/Software	
2	Form 2	Conflict of Interest	
3	Form 3	Performance Bank Guarantee	
4	Form 4	Pre- Contract Integrity Contract	
5	Form 5	Proposal Covering Letter	
6	Form 6	Checklist	
7	Form 7	Malicious Code format	
8	Form 8	Undertaking of Compliance	
9	Form 9	Non-Disclosure Agreement	
10	Form 10	Price Bid Format	

7.2.7 **Form 7: Format for Malicious Code**

<< Company Letter Head >>

MALICIOUS CODE

Proposal Ref. No.: _____ & Date: _____

To,
The CMD,
Munitions India Limited,
Corporate Office: 2nd Floor Nyati Unitree,
Contact: 020-67080400
mil-pune@munitionsindia.in

Sub: Non-Malicious Code Certificate

Sir,

1. I/We hereby certify that the hardware and the software being offered as part of the agreement does not contain any kind of malicious code (at the time of delivery) that would activate procedures to:

(a) Inhibit the desired and the designed function of the equipment.

(b) Cause physical damage to the user or his equipment during the operational exploitation of the equipment.

(c) Tap information regarding network, network users and information stored on the network that is classified and / or relating to National Security, thereby contravening Official Secrets Act 1923.

2. At the time of delivery, there are no Trojans, Viruses, Worms, Spywares or any malicious software on the system and in the software developed.

3. Without prejudice to any other rights and remedies available to Munitions India Limited, we are liable in case of physical damage, loss of information and those relating to copyright and Intellectual Property rights (IPRs), caused due to activation of any such malicious code in embedded / shipped software at the time of delivery.

Date:
Place:

Authorised Signatory:
Name of the Person:
Designation:
Firm Name & Seal:

7.2.8 Form 8: Format for Undertaking on Compliance of Technical Specifications and Tender Specifications and Terms & Conditions

<< Company Letter Head >>

I/We hereby undertake that I/we have examined/ perused, studied and understood the RFP document No. .....Dated and any corrigendum/ addendum/ clarification etc. completely and have submitted my/our bid in pursuance and without any material and/or other deviations to the said documents.

I/We hereby undertake that we shall comply with the Scope of work and requirements and tender terms and conditions completely and there are no deviations of any manner and/or sort and/or kind in this regard from my/our side.

I/WE hereby confirm that the solution and scope of work mentioned in this tender are workable proper and sustainable as per information provided in the tender document.

I/We hereby affirm that our response is valid for the period including the deemed period as specified in the tender document.

Signature of Authorized Signatory

Date

Place

Name of the Signatory

COMPANY NAME COMPANY SEAL

7.2.9 **Form 9: Format for Non-Disclosure Agreement**

<< Company Letter Head >>

NON-DISCLOSURE AGREEMENT

THIS Non-Disclosure Agreement ("Agreement") entered into on _____ (the "**Effective Date**") between:

Munitions India Limited, a Government of India Enterprise under Department of Defence Production, Ministry of Defence, Government of India, having its corporate office at 2nd Floor Nyati Unitree, Nagar Road, Yerawada, Pune - 411006, hereinafter referred to as "MIL" (hereinafter called as the "**MIL**", which expression unless repugnant to the context or meaning thereof, shall mean and include its successors or nominees or assignees or legal representative) of the FIRST PART;

And

M/s. Railtel Corporation Ltd having its corporate office at _____ (hereinafter called as "**Railtel",** which expression unless repugnant to the context or meaning thereof, shall mean and include its successors or nominees or assignees or legal representative) of the SECOND PART;

RECITALS

WHEREAS

A. MIL has inked a contract No. _____ **Date:** _____ (**Contract**) with Railtel for "SETTING UP OF DATA CENTER & DISASTER RECOVERY CENTER BASED ON INFRASTRUCTURE AS A SERVICE (IaaS) PLATFORM FOR ERP SAP S/4 HANA SYSTEM (hereinafter called as "**DC/DR Service**").

B. MIL, in furtherance of such relationship, will disclose Confidential Information (defined below);

C. Railtel shall protect and preserve the confidentiality of Confidential Information provided by the MIL to the Seller by preventing its unauthorized disclosure and use, in accordance with the terms of Contract; and

D. Railtel agrees to hold Confidential Information in strict confidence that are no less than what is agreed in the Contract, and will not disclose or use, directly or indirectly, for any purpose other than the performance of the Contract.

Railtel agree as follows: -

Confidential Information:

Railtel recognizes that during the term of the Contract, sensitive data will not be made available to its sub-contractors and agents and others working for or under Railtel without express written permission from MIL. Further, Railtel also recognizes that any improper and unauthorized disclosure or usage of DC/DR data by any such recipient may constitute a breach of applicable laws causing harm not only to MIL but also the stakeholders whose data is used. Any breach of any confidentiality obligation set out in the Contract will result in MIL a right to seek injunctive relief and damages suffered or are reasonably likely to be suffered and the cost incurred to mitigate the implication of such disclosure or usage, from Railtel.

"Confidential Information" means any and all information that is or has been received by Railtel (the "Receiving Party") from MIL (the "Disclosing Party") or that: (a) relates to the Disclosing Party; and (b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or (c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.

"Confidential Materials" shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and server disks or tapes, whether machine or user readable.

Managing Confidential Information:

The Receiving Party agrees to regard, preserve and keep as confidential all confidential information and materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:

(a) Disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, Company or any other entity other than its directors, partners, advisers, agents or employees. The Receiving Party agrees to be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees is in accordance with the terms and conditions of this Contract; or

(b) Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers.

In maintaining confidentiality hereunder, the Receiving Party on receiving the Confidential Information and materials agrees and warrants that it shall:

(a) Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own Confidential Information of like importance and such degree of care shall be at least that which is reasonably calculated to prevent such inadvertent disclosure.

(b) Keep the Confidential Information and materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party.

(c) Upon discovery of any unauthorized disclosure of Confidential Information, promptly inform the MIL of such disclosure in writing and immediately return to the MIL all such Information and materials, in whatsoever form, including any and all copies thereof.

The restrictions in this Para shall not apply to:

(a) Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this Contract); or

(b) Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any inquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure; or

The Receiving Party agrees that its obligation under this Section with respect to confidentiality will survive the termination of this Contract.

Confidential Information shall be and remain the property of the MIL and nothing in this Contract shall be construed to grant either Party any right or license with respect to the other Party's Confidential Information otherwise than as is expressly set out in this Contract.

The restrictions in this Para shall not apply to:

(a) Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this Contract); or

(b) Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any inquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the

Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure; or

D. Term

Railtel agrees that this undertaking will be effective from the date of execution of the Contract and shall continue even after the end of their assignment with MIL, for perpetuity.

E. Dispute Resolution:

The Parties agree that the laws of India will govern this Agreement

At the first instance all the disputes or claim concerning the interpretation or application of the Contract signed between MIL and RailTel shall be settled amicably by mutual discussions between the authorized representatives of the Parties.

In the event that any dispute or difference relating to the interpretation and application of the provisions of this Agreement is not settled amicably, such dispute or difference shall be taken up by either party for resolution through AMRCD as mentioned in DPE OM No. 05/0003/2019-FTS-10937 dated 14/12/2022 as amended from time to time, and the decision of AMRCD on the said dispute shall be binding on both the parties.

The Parties shall not be released from performing their obligations hereunder by reason of any dispute resolution proceedings being instituted.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE EXECUTED THIS CONFIDENTIALITY AGREEMENT IN DUPLICATE BY AFFIXING THE SIGNATURES AS OF THE DATE HEREIN ABOVE MENTIONED.

For MIL	**For Railtel**
_____	_____
Name:	**Name:**
Designation:	**Designation:**

7.2.10 Form 10: Price Bid Format

Sr. No.	Item	Description	Basic Price	GST on Basic Price (a)	Total Price [(a) + (b)]
			(a)	(b)	(c)
1	Service Charges per Quarter	Service Charges per Quarter for IaaS based platform for DC/DR Services			

(* Component wise cost break up to be submitted along with the main price bid as above.)

CIN No. U29190PN2021GOI203505

पंजीकृत पता: गोला बारुद निर्माणी, खड़की, पुणे, महाराष्ट्र – 411 003.

निगमनर्त कार्यालय पता: दूसरी रंनजल, त्रानत रूनिट्री, िगर रोड, रेरवडा, पुणे - 411 006

Regd. Address: Ammunition Factory, Khadki, Pune, Maharashtra – 411 003.

Corporate Office Address: 2nd Floor, Nyati Unitree, Nagar Road, Yerwada, Pune – 411 006

दूरभाष सं / PHONE No. 020-67080400,

Email: mil-pune@munitionsindia.in

Web Address: https://munitionsindia.in