PETROLEUM AND EXPLOSIVES SAFETY ORGANIZATION (PESO),
DEPARTMENT FOR PROMOTION OF INDUSTRY AND INTERNAL TRADE
MINISTRY OF COMMERCE AND INDUSTRY, GOVERNMENT OF INDIA

REQUEST FOR PROPOSAL
FOR SELECTION OF
MANAGED SERVICES PROVIDER (MSP)
FOR HIRING OF CLOUD SERVICES
FOR MIGRATION AND HOSTING OF PESO APPLICATIONS

11th September, 2026

Table of Contents

Content
Summary
Disclaimer
Section 1. Letter of Invitation
1.1 Introduction
1.2 Duration of engagement
Section 2. Instructions to Applicants
2.1 Introduction
2.2 Clarification and amendment of RFP documents
2.3 Earnest Money Deposit
2.4 Preparation of proposal
2.5 Submission, receipt and opening of proposals
2.6 Proposal Evaluation
2.7 Terms & Conditions
2.8 Appointment of Agency
2.9 Performance Guarantee
2.10 Exit Management and Knowledge Transfer
2.11 Failure to Agree with the Terms and Conditions of the RFP
2.12 Resolution of Disputes
2.13 Miscellaneous
2.14 Tentative schedule for selection process
Section 3. Pre-Qualification and Technical Proposal - Standard Forms
Section 4. Financial Proposal - Standard Forms
Section 5. Scope of Work
Section 6. Delivery Schedule/Timelines
Section 7. Deliverables & Timelines
Section 8. Standard Form of Work Order
Annexure A: Form of Bank Guarantee for Performance Security
Annexure B: Technical Requirements – Cloud Service Provider

Annexure C: Publicly Listed Prices of CSP
Annexure D - Financial Bid Format Final

PETROLEUM AND EXPLOSIVES SAFETY ORGANIZATION (PESO),
DEPARTMENT FOR PROMOTION OF INDUSTRY AND INTERNAL TRADE

REQUEST FOR PROPOSAL (RFP) FOR SELECTION OF MANAGED SERVICES PROVIDER (MSP)
FOR HIRING OF CLOUD SERVICES
FOR MIGRATION AND HOSTING OF PESO APPLICATIONS

1. The Petroleum and Explosives Safety Organization (PESO), formerly known as Department of Explosives, a statutory safety Organisation under Department for Promotion of Industry and Internal Trade, since its inception on 05/09/1898, has been serving the nation as a nodal agency for regulating safety of hazardous substances such as explosives, compressed gas and petroleum. PESO's major work is to administer the responsibilities delegated under the Explosives Act 1884 and Petroleum Act 1934 and the Rules made thereunder related to manufacture, import, export, transport, possession, sale and use of Explosives, Petroleum products and Compressed gases.

2. The Petroleum and Explosives Safety Organisation, functioning under DPIIT, is the statutory authority responsible for administering regulatory functions relating to explosives, petroleum, compressed gases and allied hazardous substances under the applicable Acts and Rules. PESO's role is critical in ensuring public safety while enabling industrial activity across sectors dependent on explosives, petroleum products, compressed gases, gas cylinders, pressure vessels, ammonium nitrate and related infrastructure.

3. The selected MSP will be responsible for end-end successful migration of the existing PESO IT infrastructure. PESO/DPIIT will be requiring a combination of all the 3 cloud deployment models, i.e – IaaS, PaaS and SaaS. The 3 models will be utilized across various service categories like compute, storage, networking & security - IaaS, containers & databases - PaaS and Analytics & Data warehousing – PaaS/SaaS. The PESO website is deployed on an Active-Active DC/NDR Setup for High availability and near zero data loss (on physically separate Meity empanelled Data Centers) with Far DR for additional backup copy. The successful MSP is expected to provide a cloud environment that will aid in continuing with a similar highly available architecture with near zero data loss and a Far DR for backup. The other PSEO applications are currently deployed on-premises and need to be migrated to the proposed cloud.

4. The detailed scope of work, eligibility criteria, proposal submission requirements, evaluation methodology, team requirements and prescribed formats for submission are provided in this RFP document. The RFP document may be accessed on the Government e-Marketplace portal **http://gem.gov.in/** and the PESO/DPIIT website **http://peso.gov.in**, as applicable. The RFP shall be governed by the terms and conditions specified in this document.

5. Interested applicants are requested to submit their responses to this RFP on Government e-Marketplace http://gem.gov.in/ on or before 24th September 2026 at 4:00 PM. **The submissions must be addressed to:** O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in

Disclaimer

1. This RFP document is neither an agreement nor an offer by Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India (hereinafter referred to as PESO/DPIIT) to the prospective Applicants or any other person. The purpose of this RFP is to provide information to the interested parties that may be useful to them in formulating their proposal pursuant to this RFP.

2. PESO/DPIIT does not make any representation or warranty as to the accuracy, reliability or completeness of the information in this RFP document. PESO/DPIIT can't consider the particular needs of each party who reads or uses this document. RFP includes statements which reflect various assumptions and assessments arrived at by PESO/DPIIT in relation to the statement of work. Such assumptions, assessments and statements do not purport to contain all the information that each Applicant may require. Each prospective Applicant should conduct its investigations and analyses and check the accuracy, reliability and completeness of the information provided in this RFP document and obtains independent advice from appropriate sources.

3. PESO/DPIIT will not have any liability to any prospective Applicant/ Firm/ or any other person under any laws (including without limitation the law of contract, tort), the principles of equity, restitution or unjust enrichment or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with anything contained in this RFP document, any matter deemed to form part of this RFP document, the award of the Assignment, the information and any other information supplied by or on behalf of PESO/DPIIT or their employees, any Agency or otherwise arising in any way from the selection process for the Assignment. PESO/DPIIT will also not be liable in any manner, whether resulting from negligence or otherwise caused by the reliance of any Applicant upon any statements contained in this RFP.

4. PESO/DPIIT will not be responsible for any delay in receiving the proposals. The issue of this RFP does not imply that PESO/DPIIT is bound to select an Applicant or to appoint the Selected Applicant, as the case may be, for the services, and PESO/DPIIT reserves the right to accept/reject any or all of the proposals submitted in response to RFP document at any stage without assigning any reasons whatsoever. PESO/DPIIT also reserves the right to withhold or withdraw the process at any stage with intimation to all who submitted RFP Application.

5. The information given is not exhaustive on account of statutory requirements and should not be regarded as a complete or authoritative statement of law. PESO/DPIIT accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the law expressed herein.

6. PESO/DPIIT reserves the right to change, modify, amend, add to, delete or cancel any or all provisions of this RFP document. Any amendment, corrigendum or clarification issued by

PESO/DPIIT shall be uploaded on the official website of PESO/DPIIT and / or Government e-Marketplace, as applicable, and shall form part of this RFP document.

1. Section 1. Letter of Invitation

New Delhi

Date: 11th September 2026

1.1. Introduction

The Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India, invites proposals from eligible agencies for selection of Managed Services Provider (MSP) for hiring of cloud services for migration and hosting of PESO applications.

PESO/DPIIT will be requiring a combination of all the 3 cloud deployment models, i.e – IaaS, PaaS and SaaS. The 3 models will be utilized across various service categories like compute, storage, networking & security - IaaS, containers & databases - PaaS and Analytics & Data warehousing – PaaS/SaaS. The PESO website is deployed on an Active-Active DC/NDR Setup for High availability and near zero data loss (on physically separate Meity empanelled Data Centres) with Far DR for additional backup copy. The successful MSP is expected to provide a cloud environment that will aid in continuing with a similar highly available architecture with near zero data loss and a Far DR for backup. The other PSEO applications are currently deployed on-premises and need to be migrated to the proposed cloud.

The Petroleum and Explosives Safety Organisation, functioning under PESO/DPIIT, is responsible for administering regulatory functions relating to explosives, petroleum, compressed gases and allied hazardous substances under the applicable Acts and Rules. PESO's functions include approval and licensing-related administration, safety compliance, inspections, audits, accident investigation and advisory support in relation to hazardous substances

The selected agency shall function as the Managed Services Provider (MSP) for hiring of cloud services for migration and hosting of PESO applications. The selected agency shall not undertake technical validation, engineering assessment, safety certification, licensing approval, inspection, enforcement or any statutory function. All statutory functions, technical inputs and final decisions shall remain with PESO/DPIIT, or other competent authorities, as applicable.

1.2. Duration of Engagement

The contract duration is for 13 Months from the date of contract award as mentioned in the work order. Further to this, as per the user's requirement and with the consent of all stakeholders, the contract may be extended upon mutual agreement, for continuation of smooth services.

An Agency will be selected through the Quality cum Cost Based Selection (QCBS) process, as specified in this RFP. The current RFP draft follows a QCBS selection approach and includes technical and financial proposal evaluation provisions. This RFP includes the following documents: -

SECTION 1: Letter of Invitation

SECTION 2: Instructions to applicants

SECTION 3: Pre - Qualification and Technical Proposal - Standard Forms

SECTION 4: Financial Proposal - Standard forms

SECTION 5: Scope of Work

SECTION 6: Delivery Schedule/Timelines

SECTION 7: Deliverables & Timelines

SECTION 8. Standard Form of Work Order

All clarifications/ corrigenda will be published only on the website of PESO/DPIIT. The official website for accessing the information related to RFP is: https:// PESO/DPIIT.gov.in/ (the "Official Website") along with Government E Marketplace (http://gem.gov.in/).

Yours Sincerely,

HoD/ Chief Controller of Explosives

PESO

2. Section 2. Instructions for Applicants

2.1 Introduction

2.1.1 The Client named in the Data Sheet will select an organization in accordance with the method of selection specified in the Data Sheet. Applicants are advised that the selection of Agency shall be, on the basis of an evaluation by Client through the selection process specified in this RFP (the Selection Process). Applicants shall be deemed to have understood and agreed that no explanation or justification for any aspect of the Selection Process will be given and that Client's decisions are final without any right of appeal whatsoever.

2.1.2 The Applicants are **invited to submit Technical and Financial Proposals (collectively called as - the Proposal),** as specified in the Data Sheet, for the services required for the Assignment. The Proposal will form the basis for grant of a work order to the selected Agency. The Agency shall carry out the assignment in accordance with the **Terms of Reference** of RFP (the - TOR).

2.1.3 The Applicant shall submit the Proposal in the form and manner specified in this RFP. The Proposal shall be submitted per the forms given in the relevant sections.

2.1.4 Applicants shall bear all costs associated with the preparation and submission of their proposals, and their participation in the Selection process, and presentation, including but not limited to postage, delivery fees, and expenses associated with any demonstrations or presentations which may be required by Client or any other costs incurred in connection with or relating to its Proposal. The Client is not bound to accept any Proposal and reserves the right to annul the selection process at any time prior to the grant of work order, without thereby incurring any liability to the Applicants.

2.1.5 Client requires that the Applicant hold Client's interest's paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The applicant shall not accept or engage in any assignment that may place it in a position of not being able to carry out the assignment in the best interests of Client and the Project.

2.1.6 It is the Client's policy to require that the Applicants observe the highest standard of ethics during the Selection Process and execution of work/assignment. In pursuance of this policy, the Client:

(i) will reject the Proposal for award if it determines that the Applicant has engaged in corrupt or fraudulent activities in competing for the work order in question;
(ii) will declare an Applicant ineligible, either indefinitely or for a stated period of time, to be awarded any contract or work order if it at any time determines that the Applicant has engaged in corrupt or fraudulent practices in competing for and in executing the work order.

2.1.7 **Dispute Resolution:** If any dispute or difference of any kind whatsoever arises between the parties in connection with or arising out of or relating to or under this RFP, the parties shall promptly and in good faith negotiate with a view to its amicable resolution and settlement. In the event no amicable resolution or settlement is reached within a period of thirty (30) days from the date on which the above-mentioned dispute or difference arose, such dispute or difference shall be finally settled by the Secretary, PESO/DPIIT, whose decision shall be final.

2.1.8 **Termination of Assignment:** Client will have the right to terminate the assignment by giving

30 (thirty) days written notice. In the event of termination for no fault of Applicant, the Client will reimburse all the expenses incurred by the Applicant (upon submission of proof), including closing-up of the project. If the assignment is terminated due to the fault of the Applicant or in case of termination of the assignment by the Applicant for reasons not attributable to the Client, the Client will forfeit the performance security of the Applicant.

2.1.9 The Applicants shall submit their proposal in four covers containing details of Earnest Money Deposit (EMD) or Bid Securing Declaration, Pre-Qualification Proposal, Technical Proposal and Financial Proposal through Government e-Marketplace (GeM) Portal (https://gem.gov.in/). Original EMD or Bid Securing Declaration is to be deposited at PESO/DPIIT. No proposal shall be accepted in any other form and shall be summarily rejected.

2.1.10 The evaluation will be done in accordance with procedure given in Clause 2.6.

2.1.11 Number of Proposals: No Applicant shall submit more than one Application.

2.1.12 Right to reject any or all Proposals:

(i) Notwithstanding anything contained in this RFP, the Client reserves the right to accept or reject any Proposal and to annul the Selection Process and reject all Proposals, at any time without any liability or any obligation for such acceptance, rejection or annulment, and without assigning any reasons thereof.

(ii) Without prejudice to the generality of above, the Client reserves the right to reject any Proposal if:

a) at any time, a material misrepresentation is made or discovered, or
b) the Applicant does not provide, within the time specified by the Client, the supplemental information sought by the Client for evaluation of the Proposal.

(iii) Such misrepresentation/ improper response by the Applicant may lead to the disqualification of the Applicant. If such disqualification/ rejection occurs after the Proposals have been opened and the highest-ranking Applicant gets disqualified/ rejected, then the Client reserves the right to consider the next best Applicant or take any other measure as may be deemed fit in the sole discretion of the Client, including annulment of the Selection Process.

2.1.13 **Acknowledgement by Applicant** - It shall be deemed that by submitting the Proposal, the Applicant has:

a. made a complete and careful examination of the RFP;
b. received all relevant information requested from the Client;
c. accepted the risk of inadequacy, error or mistake in the information provided in the RFP or furnished by or on behalf of the Client;
d. satisfied itself about all matters, things and information, including matters herein above, necessary and required for submitting an informed Application and performance of all of its obligations there under;
e. acknowledged that it does not have a Conflict of Interest; and
f. agreed to be bound by the undertaking provided by it under and in term hereof.

The Client and/ or its advisors shall not be liable for any omission, mistake or error on the part of the Applicant in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP or the Selection Process, including any error or mistake therein or in any information or data given by the Client and/ or its consultant.

2.2 Clarification and amendment of RFP documents

Applicants may seek clarification on this RFP document, within Four (4) days of the date of issue of this RFP document. Any request for clarification must be sent by standard electronic means (PDF and word file) to the Client's email addressed: expl-dipp@nic.in. The Client will endeavour to respond to the queries prior to the Proposal Due Date. The Client will post the reply to all such queries on its official website and GeM portal.

2.2.1 At any time before the submission of Proposals, the Client may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Applicant, modify the RFP documents by amendment. Only the amendments/corrigenda posted on the Client's Official Website shall be valid. In order to afford the Applicants a reasonable time for taking an amendment into account, the Client may at its discretion extend the Proposal Due Date.

2.2.2 Date of Pre-Bid Meeting and venue is mentioned in Data Sheet. Applicants willing to attend the pre-bid should inform client beforehand in writing through email. The maximum no. of participants from an applicant, who chose to attend the Pre-Bid Meeting, shall not be more than two per applicant. The representatives attending the Pre-Bid Meeting shall accompany with an authority letter duly signed by the authorized signatory of his/her organization

2.3 Earnest Money Deposit

2.3.1 An EMD (Earnest Money Deposit) in the form of a Demand Draft/ Bank Guarantee, from a scheduled Indian Bank in Favor of Pay and Account Officer, PESO/DPIIT, New Delhi, payable at New Delhi, for the sum INR 75,00,000/- (Rupees Seventy-Five Lakhs only) shall be required to be submitted by each Applicant. The Bank Guarantee shall be in the format of Form 3C.

2.3.2 The Demand Draft/ Bank Guarantee in original shall be placed in an envelope and marked as -EMD- [name of assignment] and -Not to be opened except in the presence of evaluation committee. This envelope shall be delivered to PESO/DPIIT in physical form before the Proposal Due Date. In addition, a scanned copy (in pdf format) shall also be uploaded on GEM. Bids received without the specified Earnest Money Deposit Bid Security will be summarily rejected.

2.3.3 Alternative to Earnest Money Deposit: In lieu of submission of EMD as stipulated in section 2.3.1 above, applicants are hereby granted a choice to submit a Bid Securing Declaration (on a notarized Rs. 100/- Stamp Paper) in accordance with Rule 170 (iii) of GFRs, 2017 concerning alternatives to Earnest Money Deposits (reproduced below).

Rule 170 (iii): In place of a Bid security, the Ministries/ Departments may require Bidders to sign a Bid securing declaration accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for the period of time specified in the request for bids document from being eligible to submit Bids for contracts with the entity that invited the Bids.

2.3.4 Client will not be liable to pay any interest on Earnest Money Deposit. Bid security of Pre-Qualified but unsuccessful Applicants shall be returned, without any interest, within one month after grant of the work order to the Selected Applicant or when the selection process is cancelled by Client. The Selected Applicant's Earnest Money shall be returned, without any interest upon the Applicant accepting the work order and furnishing the Performance in accordance with provision of the RFP and work order.

2.3.5 Client will be entitled to forfeit and appropriate the Earnest Money Deposit as mutually agreed loss and damage payable to Client in regard to the RFP without prejudice to client's any other right or remedy under the following conditions:

(i) If an Applicant engages in a corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice as envisaged under this RFP (including the Standard Form of work order);

(ii) If any Applicant withdraws its Proposal during the period of its validity as specified in this RFP and as extended by the Applicant from time to time,

(iii) In the case of the Selected Applicant, if the Selected Applicant fails to accept the work order or provide the Performance Security within the specified time limit, or

(iv) If the Applicant commits any breach of terms of this RFP or is found to have made a false representation to Client.

Performance Security equivalent to the amount indicated in this RFP shall be furnished before start of work on assignment in form of a Bank Guarantee substantially in the form specified in the RFP/ work order.

For the successful bidder the Performance Security shall be retained by Client until the completion of the assignment by the Applicant and be released 60 (Sixty) days after the completion of the assignment.

2.3.6 Any entity which has been barred by the Central Government, any State Government, a statutory authority or a public sector undertaking, as the case may be, from participating in any project and the bar subsists as on the date of the Proposal Due Date, would not be eligible to submit a Proposal.

2.3.7 An Applicant should have, during the last 3 (three) years, neither failed to perform on any agreement, as evidenced by imposition of a penalty by an arbitral or judicial authority or a judicial pronouncement or arbitration award against the Applicant or its Associate, nor been expelled from any project or agreement nor have had any agreement terminated for breach by such Applicant or its Associate.

2.4 Preparation of proposal

2.4.1 Applicants are requested to submit their Proposal in English language and strictly in the formats provided in this RFP. The Client will evaluate only those Proposals that are received in the specified forms and complete in all respects.

2.4.2 In preparing their Proposal, Applicants are expected to thoroughly examine the RFP Document.

2.4.3 The technical proposal should provide the documents prescribed in this RFP. No information related to financial proposal should be provided in the technical proposal.

2.4.4 Failure to comply with the requirements spelt out above shall lead to the deduction of marks during the evaluation. Further, in such a case, Client will be entitled to reject the Proposal. However, if any information related to financial proposal is included in the technical proposal the applicant shall be disqualified and his proposal will not be considered.

2.4.5 The Proposals must be digitally pre-signed by the Authorized Representative (the-Authorized Representative) as detailed below:

(i) by the proprietor in case of a proprietary firm;

(ii) by a partner, in case of a partnership firm and/or a limited liability partnership; or

(iii) by a duly authorized person holding the Power of Attorney, in case of a Limited Company or a corporation;

2.4.6 Applicants should note the Proposal Due Date, as specified in Data Sheet, for submission of Proposals. Except as specifically provided in this RFP, no supplementary material will be entertained by the Client, and the evaluation will be carried out only on the basis of Documents received by the closing time of Proposal Due Date as specified in Data Sheet. Applicants will ordinarily not be asked to provide additional material information or documents subsequent to the date of submission, and unsolicited material if submitted will be summarily rejected. For the avoidance of doubt, the Client reserves the right to seek clarifications in case the proposal is non- responsive on any aspects.

2.4.7 Financial proposal: While preparing the Financial Proposal, Applicants are expected to take into account the various requirements and conditions stipulated in this RFP document. The Financial Proposal should be a lump sum Proposal inclusive of all the costs including GST applicable. While submitting the Financial Proposal, the Applicant shall ensure the following:

(i) All the costs associated with the Assignment shall be included in the Financial Proposal. These shall normally cover remuneration for all the personnel (Expatriate and Resident, in the field, office, etc.), local transportation at the location of deployment, equipment, printing of documents, secondary and primary data collection, etc. The total amount indicated in the Financial Proposal shall be without any condition attached or subject to any assumption, and shall be final and binding. In case any assumption or condition is indicated in the Financial Proposal, it shall be considered non-responsive and liable to be rejected.

(ii) The Financial Proposal shall take into account all the expenses and cost of insurance specified in the work order, levies and other impositions applicable under the prevailing law. Further, all payments shall be subjected to deduction of taxes at source as per Applicable Laws.

2.4.8 The proposal should be submitted as per the standard Financial Proposal submission forms prescribed in this RFP.

2.4.9 Applicants shall express the price of their services in Indian Rupees only.

2.4.10 The Financial proposal of the technically qualified participating agencies will be opened by the Committee on the prescribed date in the presence of the Agency's representatives. The names of technically qualified participating agencies with their overall technical scores shall be uploaded on the GeM Portal.

2.5 Submission, receipt and opening of proposals

2.5.1 The Proposal shall be submitted through the GeM portal. The procedure for filing of e-tender is provided on the portal. Files uploaded on the portal should have file name in accordance to the following format [form_name.applicant_name]. Applicant name should contain only first two words of its name.

2.5.2 The Authorized Representative of the Applicant should authenticate EMD Details, Pre-qualification, Technical and Financial proposal using digital signatures. The Authorized Representative's authorization should be confirmed by a written power of attorney by the competent authority accompanying the Proposal (Pre-Qualification Proposal).

2.5.3 The Applicant shall submit his proposal in four covers containing details of EMD, Pre-Qualification Proposal, Technical Proposal and Financial Proposal respectively, through GeM portal.

2.5.4 No proposal shall be accepted after the closing time for submission of Proposals. After the deadline for submission of proposals the Pre-Qualification Proposal shall be opened by the Evaluation Committee to evaluate whether the Applicants meet the prescribed Minimum Qualification Criteria. The RFP, Technical and Financial Proposals shall remain sealed.

2.5.5 After the Proposal submission until the grant of the work order, if any Applicant wishes to contact the Client on any matter related to its proposal, it should do so in writing at the Proposal submission address. Any effort by the firm to influence the Client during the Proposal evaluation, Proposal comparison or grant of the work order decisions may result in the rejection of the applicant's proposal.

2.6 **Proposal Evaluation**

2.6.1 As part of the evaluation, the Pre-Qualification Proposal submitted (Form 3A - 3B) shall be checked to evaluate whether the Applicant meets the prescribed Minimum Qualification Criteria. Subsequently the Technical Proposal submission, for Applicants who meet the Minimum Qualification Criteria (-Shortlisted Applicant), shall be checked for responsiveness in accordance with the requirements of the RFP and only those Technical Proposals which are found to be responsive would be further evaluated in accordance with the criteria set out in this RFP document.

2.6.2 Prior to evaluation of Proposals, the Client will determine whether each Proposal is responsive to the requirements of the RFP at each evaluation stage as indicated below. The Client may, in its sole discretion, reject any Proposal that is not responsive hereunder. A Proposal will be considered responsive at each stage only if the following requirements are met:

I. Pre-qualification

The client will satisfy itself that the applicants meet the minimum qualifications prescribed before evaluating technical and financial proposals.

II. Technical Proposal

a. The Technical Proposal is received in the form specified in this RFP;

b. It is accompanied by the Earnest Money Deposit (or Bid Securing Declaration) as specified in this RFP;

c. It is received by the Proposed Due Date, including any extension thereof in terms thereof;

d. It does not contain any condition or qualification; and

e. It is not non-responsive in terms hereof.

III. Financial Proposal

a. The Financial Proposal is received in the form specified in this RFP;

b. It is received by the Proposed Due Date including any extension thereof, in terms hereof;

c. It does not contain any condition or qualification; and

d. It is not non-responsive in terms hereof.

The Client reserves the right to reject any Proposal which is non-responsive and no request for alteration, modification, substitution or withdrawal will be entertained by the Client in respect of such Proposals. However, client reserves the right to seek clarifications or additional information from the applicant during the evaluation process. The Client will subsequently examine and evaluate Proposals in accordance with the Selection Process detailed out below. As part of the evaluation, the Pre-Qualification Proposals submitted should fulfill the Minimum Qualification Criteria. In case an Applicant does not fulfill the Minimum Qualification Criteria, the Proposal of such an Applicant will not be evaluated further.

2.6.3 Pre-Qualification Criteria (PQC)

Eligibility of the Proposed Managed Service Provider (MSP):

Sr. No	Requirements	Documents to be submitted
1	a) Bidder must be a Legal Entity i.e., a company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013/ Partnerships Firm registered under the Limited Liability Partnerships or Partnership Act. AND b) Registered with the Income Tax (TAN/PAN) and GST (GSTN) Authorities in India with active status **Consortium or JV not allowed.**	Certified by Authorized Signatory: 1. Copy of Certificate of Incorporation/ Registration issued by Registrar of Company (RoC). 2. Copy of GST Registration Certificate issued to bidder.
2	**The Bidder should be operating in India for at least 5 years as on the last date of bid submission.**	Documentary evidence in support of this shall be submitted.
3	The bidder shall be an **authorized Managed Service Partner (MSP) / Channel Partner of** the **MeitY-empanelled Cloud Service Provider**, for at least four **(4) years** as on the date of publication of the bid.	1. CSP's MeitY empanelment certificate. 2. Copy of Authorised partner certificates from Cloud Service Provider, signed by authorized signatory.

		3. Authorization letter from the proposed CSP for bid submission against this BID. 4. Authorization for the person signing and submitting the Bid.
4	Bidder should have Registered office in Delhi NCR Region to provide quick support and coordination during the contract duration.	Self-declaration signed by bidder's authorized signatory on company letterhead with proof of office address.
5	The Bidder shall have an annual turnover of an average INR 50 Cr from cloud Services in the last 3 audited financial years (FY 2022-2023, FY 2023-2024 & FY 2024-25).	Copy of audited statement of account (P&L account & Balance Sheet) or CA Certificate duly certified by the Statutory Auditor/ Chartered Accountant holding a certificate of practice and containing a valid UDIN along with a certificate stating the Cloud turnover.
6	The bidder should have positive Net worth for the last three audited financial years (FY 2022-2023, FY 2023-2024 & FY 2024-25).	Copy of audited statement of account (P&L account & Balance Sheet) or CA Certificate duly certified by the Statutory Auditor/ Chartered Accountant holding a certificate of practice and containing a valid UDIN along with a certificate stating the Cloud turnover.
7	Bidder shall not be blacklisted/debarred by any state or central government or their agencies and should not have been found guilty of any criminal offence by any court of law, in the last three (3) years as on the date of the bid publication.	Self-declaration from Bidder on his letterhead.
8	The bidder should have experience in implementing similar Cloud Management projects (i.e. having at least compute, storage, network, security, database, and management services) with the proposed Cloud Services provider for Central or State Government departments, ministries, PSUs in the last 5 years ending 31st March 2026. Project should have completed at least 1 year billing cycle. * at least one (01) clients for work order value of ₹ 21 crores each. * at least two (02) clients for work order value of ₹ 10.5 crores each.	Copy of Work Order + Completion Certificate /client satisfactory letter.

	* at least three (03) clients for work order value of ₹ 7 crores each.	
9	The bidder must possess: i) ISO/IEC 20000-1:2018 ii) ISO 9001:2015 or latest iii) ISO/IEC 27001:2022 iv) CMMi Level 3 and above	Self-certified copies of certificates, obtained from certifying authorities (validity at the time of the bidding process)
10	The bidder should have a minimum of 20 certified cloud resources on their payroll. Certifications should be valid as on the date of bid submission.	Certified by Company Secretary/ HR along with valid CSP certification along with relevant certificate types.
11	The bidder must also furnish the Manufacturer's Authorization Form (MAF) for any third party security components, as required	MAF from 3rd party security OEM
12	EMD 6. **The Bidder must submit a **refundable** Earnest Money deposit (EMD) of INR 75,00,000/- (Rupees Swenty Five Lakhs only) in Indian Rupees in the form of NEFT/RTGS NEFT details given below: Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in.	Copy of Receipt attached as per Form 3C.

Pre-Qualification Criteria for CLOUD SERVICE PROVIDER (CSP)

S.No.	Description	Supporting Document
1	The Cloud Service Provider (CSP) should have at least 4 Data Center locations in minimum 2 different cities empaneled for both public cloud and VPC, with minimum 03 years of Meity empanelment.	Bidder to submit self Declaration on CSP Letterhead. Miety empanelment certification of CSP.
2	The Meity empaneled DC and the Far DRC of the Cloud Service Provider (CSP) should be in different seismic zones.	Bidder to submit self-Declaration on CSP Letterhead.
3	The Cloud Service Provider (CSP) shall have the capability to provide an Active-Active DC-NDR with synchronous replication providing near zero data loss capability. Each data center offered for DC/NDR should be separately empaneled by Meity.	Bidder to submit self-Declaration on CSP Letterhead.
4	CSP must have an average annual turnover of not less than Rs 500 Crore for the last three consecutive financial years (2022-23, 2023-24, 2024-25) from Cloud Services.	CA Certified Turnover Certificate

5	CSP shall have published on its public-facing website-cloud services' Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global Data Centre and outage details (if any) with RCA.	An undertaking from the CSP with the links (URLs) to its relevant public facing website(s) covering the details.
6	The Cloud Service Provider (CSP) should also have the availability of self-service cloud portal and Command Line interface for managing cloud resources. CSP's Data Centre/ DRC should be a minimum of Tier III/TIA942 classification	Undertaking on CSP letterhead with a link (URL) to the public-facing website having the service and functionality description. TIER III/TIA942 certificate
7	The Cloud Service Provider (CSP) should have native Machine Learning capabilities, including support for Serverless AI Inference and managed training workflows, enabling users to automatically select the best model and hyperparameters for their data. The CSP should also have capability for seamless integration with native DevOps for operationalizing machine learning models. The CSP must have frontier AI models hosted in India for within country inferencing.	Undertaking on CSP letterhead with link (URL) to public facing website having the service and functionality description.
8	The CSP facilities/services need to be certified / compliant to the following standards: a. ISO 27001 - Data Centre and the cloud services should be certified for the latest version of the standards -.ISO/IEC 27017:2015-Code of practice for information security controls b. ISO 27701 - international standard that acts as a Privacy Information Management System (PIMS) extension to ISO/IEC 27001 c. ISO 27017 - standard providing guidelines for information security controls in cloud services d. ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds. e. ISO 20000-1-Guidance on the application of ISO/IEC to cloud services. f. ISO 22301 - international standard for Business Continuity Management Systems (BCMS), providing a framework to help organizations identify threats, protect against, respond to, and recover from disruptive incidents g. ISO/IEC 42001- framework for managing the risks and opportunities associated with artificial intelligence, including ethics, transparency, and accountability h. PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card	Copy of Certification/self-declaration (where applicable)

	information in the cloud – This standard is required if the transactions involve credit card payments. i. SOC 1/2/3 Compliance	
9	CSP compute services should offer any of three (03) different processor architecture support Viz. Intel x86, AMD & ARM based computer services. These services offering should also be available for managed compute services for database, caching, etc.	Undertaking on CSP letterhead with link (URL) to public facing website having the service and functionality description.
10	CSP should be able to offer Native PaaS services on content delivery service for delivery of live services across country and across the world.	Self-certified certification from the CSP.
11	CSP must have native managed databases capability for both MS SQL Server and PostGreSQL.	Self-certified certification from the CSP.
12	The CSP must be able to offer managed In-Country AI Model Inferencing and Data Residency. The Inference processing, prompts and responses processed should reside within Meity empanelled Data centres in India. The CSP must be able to offer at least 5 frontier LLMs available for in-country inferencing	Self-certified certification from the CSP.

2.6.4 Technical Qualification Criteria (TQC)

The Technical Evaluation Committee appointed by the PESO/DPIIT will carry out the evaluation of Proposals on the basis of the following evaluation criteria and points system. If required, the Client may seek specific clarifications from any or all Agency at this stage. Each evaluated Proposal will be given a technical score as detailed below. The maximum points/ marks to be given under each of the evaluation criteria are:

Sr. No	Parameters	Specification	Documentary evidence	Max Mark
1	The Bidder shall have an annual turnover of an average INR 50 Cr from Cloud business in the last 3 audited financial years (FY 2022-2023, FY 2023-2024 & FY 2024-25).	Equal or more than 50 Cr and Less than 75 Cr: 2 **Marks** Equal or more than 75 Cr and Less than 125 Cr: 5 **Marks** Equal or more than 125 Cr: **10 Marks**	Copy of audited statement of account (P&L account & Balance Sheet) or CA Certificate duly certified by the Statutory Auditor/ Chartered Accountant holding a certificate of practice and containing a valid UDIN along with a certificate stating the Cloud turnover.	**10**
2	Cloud-certified manpower on the payroll of the	a) >=20 to < 30 cloud-certified resources– 1 **Marks**	Certified by Company Secretary/ HR along with valid CSP certification	**10**

	Bidder for last at least 12 months (The manpower should be from the proposed CSPs only)	b) >=30 to < 40 cloud-certified resources – 2 **Marks** b) 40 or more cloud-certified resources – 5 **Marks** **5** additional marks will be awarded if out of the total resources, 05 (five) resources have advanced professional certificates (ie. Architect, Security, DevOps etc.)	along with certificate types.	
3	The Bidder should be an authorized partner of MeitY empanelled Proposed CSPs. The award of marks will be carried out for the minimum association with either of the CSPs)	>=4 Years & <5 years - 2 **Marks** >=5 years - 5 **Marks** **5** additional marks to be given to the bidder having the top tier partnership with proposed CSP The MSP shall submit a letter from the proposed CSP confirming their top-tier/highest-level partnership status (e.g., Premier/Advanced/Strategic Partner) as on the date of bid submission	1. CSP's MeitY empanelment certificate. 2. Copy of Authorised partner certificates from Cloud Service Provider, signed by Authorized signatory. 3. Authorization letter from the CSP	**10**
4	The bidder should have experience in implementing similar Cloud Management projects (i.e. having at least compute, storage, network, security, database, and management services) with the proposed Cloud Services provider for central or state government departments, ministries, PSUs in the last 5 years ending 31st Mar 2026. Project should have completed at least 1 year billing cycle.	Experience in similar assignments (successfully completed) (Maximum 5 citations to be submitted) a) 1 project of value > Rs. 21 crores - 9 Marks. For each additional project/Citations – 6 Marks b) 2 projects of value > Rs.10.5 crores and <= 21 Crores - 9 Marks. For each additional project/Citations – 3 Marks. c) 3 projects of value > Rs. 7 crores and <=10.5 Crores - 9 Marks. For each additional project/Citations – 1.5 Marks.	Purchase Order copy/Work Order / LOA/ copy of contract clearly highlighting the Scope of Work, Bill of Material, value of work order/ contract along with last 12 months billing. The bidder can also attach: Certificate of Completion (if available) /Ongoing ((if available, Certified by the Statutory Auditor/Company Secretary) OR Completion Certificate (if available) issued and signed by the competent authority of the	15

			customer on letterhead OR Copies of payments received, signed by the Statutory Auditor/Company Secretary of the Bidder or any other document certifying the status of the project	
	Bidders support matrix in supporting PESO project which should cover- 1. SLA abidance 2. Support team 3. How bidder's support team will manage the escalation with escalation matrix? 4. OEM support available to support PESO 5. Technical team experience		Self-certificate and a technical proposal with writeup confirming the same	**10**
5	**Technical Presentation** The presentation shall cover the **bidder's profile**, the **proposed Cloud Service Provider (CSP) profile and capabilities**, and a **scalable cloud architecture** leveraging **open-source tools and CSP-native cloud services**, in line with the tender requirements. The presentation shall also include the bidder's **cloud migration experience**, supported by **valid migration competency/partner certifications** issued by the proposed CSP, and a demonstration of **managed cloud services and server less services** as applicable to the scope of work. The customer may seek **live demonstrations and/or use-case-based/ case study of similar assignment presentations** during the technical evaluation process. Technical Presentation should also cover CSP Cloud Technology Stack, Solution Architecture, Deployment Architecture, Integration Architecture, Migration Approach and Methodology with Migration Plan for PESO applications, Migration Timelines, Cutover and Rollback strategy		Date, Time, and Venue will be informed later	**30**
6	Cloud deployment architecture for DC & NDR Confirmation by CSP		RTO and RPO is near zero = 8 Marks RTO = 15 Minutes, RPO= 15 Minutes = 4 marks RTO = 2 hrs, RPO= 15 Minutes = 2 marks	**8**

		Supporting Document: Confirmation by CSP	
7	Managed In-Country AI Model Inferencing and Data Residency	Inference processing, prompts and responses processed should reside within Meity empanelled Data centres in India – 4 marks Minimum 10 frontier LLMs available for in-country inferencing – 3 marks	**7**
Total Marks			**100**

2.6.5 Note to the Table above:

i. Documentary evidence must be submitted for each criterion and undertaking, or declaration made by the MSP must be on the company letter head and is to be signed by an authorized signatory.

ii. The Technical Evaluation Committee (TEC) appointed by PESO/DPIIT will carry out the evaluation of Bids on the basis of the above evaluation criteria and points system. Each evaluated Bid will be given a Technical Score (Ts) as detailed above.

iii. MSPs, whose bids are responsive, based on minimum qualification criteria / documents as in Pre-Qualification Criteria and technical score at least 70 marks in the (given) defined scoring mechanism would be considered technically qualified.

iv. Technical Presentation may consist of the CSP Cloud Technology Stack, Solution Architecture, Deployment architecture, Integration Architecture, migration approach and methodology, migration timelines, etc.

v. Price Bids of such technically qualified MSPs alone shall further be opened.

vi. The MSPs will be called for a detailed presentation on each of the above criteria, at a date and time provided by PESO/DPIIT, in order to facilitate a comprehensive evaluation of their respective proposals. In case of non-attendance of MSPs in the presentation, the bid shall be given '0' (zero) marks on technical evaluation.

2.6.6 Commercial Bid Evaluation

a) The Financial Bids of technically qualified MSPs will be opened on the prescribed date in the presence of MSP representatives.

b) In case of discrepancy between the words and figures quoted, the one which is quoted in words will be considered for evaluation purposes.

c) The total quoted financial bid value will be considered for evaluation.

d) The MSP with lowest qualifying financial bid (L1) will be awarded 100 score (amongst the MSPs that qualify on the basis of technical evaluation criteria. Financial Scores for other than L1 MSPs will be evaluated using the following formula:

Financial Score of a MSP (Fn) = {(Commercial Bid of L1/Commercial Bid of the MSP) X 100}

(Figures will be adjusted to two decimal places)

e) To discourage unrealistic bids, authority may require additional performance guarantee from the successful MSP. The additional performance guarantee shall be equivalent to 10% of the difference between the two lowest commercial bids.

2.6.7 Combined and Final Evaluation

The MSP will be selected, and contract be awarded on QCBS basis as per technical score and financial bid (70:30)

Technical Score of MSP (Ts)

As per the technical evaluation, the MSPs will be assigned a technical score out of a maximum of 100 points and will be normalized on a scale of 100 to obtain the Ts, using the formula given below:

Ts = Tb/Tmax * 100

Where, Ts = Normalized technical score for the MSP under consideration

Tb = Absolute technical score for the MSP under consideration

Tmax = Maximum technical score

Financial Score of MSP (Fs)

- The financial scores would be normalized on a scale of 100, with lowest score being normalized to 100 and the rest being awarded on a pro-rata basis. Such normalized scores would be considered for the purpose of QCBS based evaluation. The individual MSP's Financial Scores are normalized as per the formula below:

  Fs = Fmin/Fb * 100

  Where, Fs = Normalized Financial score for the MSP under consideration

  Fb = Absolute financial quote for the MSP under consideration

  Fmin = Minimum absolute financial quote
- The final composite score will be worked out by adding the weighted marks on technical score (Ts) and Normalized Financial score (Fn):

  Composite Score (S) = Ts * 0.7 + Fn * 0.3
- The MSP with the highest Composite Score (S) shall be considered for the award of work.

a) Scores will be calculated upto two decimal places only.
b) In the event the composite bid scores are 'tied', the MSP securing the higher technical score will be adjudicated as the Best Value MSP for award of the Project.
c) In the event the composite bid scores and technical scores are also 'tied', authority has the discretion to choose the successful MSP and such decision of the authority would be final and binding on the MSPs.

The bidder achieving the **highest Final Score (H1)** shall be ranked first and considered for the award of contract, subject to meeting all eligibility and compliance requirements.

2.6.8 Additional Conditions for Contract

The contract duration is for 13 Months from the date of contract award as mentioned in the work order. Further to this, as per the user's requirement and with the consent of all stakeholders, the contract may be extended upon mutual agreement, for continuation of smooth services.

a) Payment will be made on the basis of actual usage of the services. The period for which services will not be availed, shall not be paid.

b) The incidental expenses of execution of agreement/contract shall be borne by the selected agency. The MSP will provide services as per PESO's requirements.

c) The vendor should provide an escalation matrix for problem resolution to PESO/DPIIT by providing the Names, Designations, Contact Number(s) and Email ID's of the persons to be contacted. The agency should also provide website URL for such purpose. The selected agency must honor all tender conditions and adherence to all aspect of fair-trade practices in executing the purchase orders placed by PESO/DPIIT. Failing this, PESO/DPIIT may forfeit their PBG and stop further participation of such agency for three years in PESO/DPIIT tendering process.

d) In the event, the vendor company or the concerned division of the Company is taken over /bought over by another company, all the obligations and execution responsibilities under the agreement with PESO/DPIIT, should be passed on for compliance by the new company in the negotiation for their transfer.

e) At any time, during the contract period, PESO/DPIIT may ask the agency to submit the supporting documents which may be required to ensure that the tender terms and conditions are fulfilled.

f) The agency should not assign or sublet the work or any part of it to any other agency. Any such attempt shall result in termination of contract and forfeiture of the PBG.

g) PESO/DPIIT may, at any time, terminate the contract by giving written notice to the vendor without any compensation, if the vendor becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to PESO/DPIIT.

h) On getting written communication from PESO/DPIIT for having qualified for award of contract, the MSP shall provide acceptance and sign the contract within 7 days of such communication. Failing which the offer shall be treated as withdrawn.

i) After selection procedure for issuance of Work Order / Purchase Order will be at the sole discretion of PESO/DPIIT. The MSP will provide services as per PESO/DPIIT requirements.

j) During the contract, PESO/DPIIT may ask the agency to submit the supporting documents which may be required to ensure that the tender terms and conditions are fulfilled.

k) PESO/DPIIT reserves the right to utilize the discovered prices of the CSP services for any additional workload of PESO/DPIIT, applicable across various missions and departments with no price increase subject to commercial contract terms.

l) The selected agency should not assign or sublet the contract or any part of it to any other agency in any form. Any such attempt shall result in termination of contract and forfeiture of the security deposit, revocation of bank guarantees (including the ones submitted for other work orders)

m) Reasons for rejecting a tender/bid will be disclosed to a MSP only where enquiries are made.

2.7 Terms & Conditions:

1. PESO/DPIIT is free to opt for any service or configuration of service in the host of offerings of the CSP at the same rate of discount.
2. The bidder is required to update the list prices in the table format provided.

3. For CSP whose list prices are in USD, RBI reference rate for USD INR conversion as on xx.xx.2026 will be taken into consideration for evaluation. (1USD = xx INR)
4. For any service, which is mentioned or not mentioned in the BOQ (including any new cloud service introduced by the CSP after the tender due date), will have to be provided to PESO at the same discount rate* as quoted in the table for the overall category.
5. PESO/DPIIT, as part of the transparent evaluation process will publish the complete details of the services submitted by all the bidders (against the different line items in the commercial bid including the price)
6. Payment
    a) Payment during development, till Go-live phase will be done based as per Payment Milestones defined in Section 6 of this document.
    b) Payment post go-live will be done on actual consumption of cloud services, as per Payment Milestones defined in Section 6 of this document. The rates of these services will be based on the discounted price as mentioned in Point 5.
7. PRICES VARIATION CLAUSE (PRICE ESCALATION/ DE-ESCALATION):
    a) Bidders are requested to offer their best discounts over the Published/Listed Rates of their CSP as on date of the tender
    b) These Discounts shall form part of Escalation/ De-escalation clause and would remain FIRM for the entire contract period.
    c) Price escalation/de-escalation shall be determined every month, based on the prevailing Published/Listed Rates in the month for which escalation is being calculated. In case the Published/Listed Rates of the respective CSP are in USD, then such rates would be converted into INR based on the published RBI reference rate of the day prior to the billing date by the MSP.
    d) Thus, the price applicable for any service in any month would be equal to Published/Listed Rates as declared by respective CSP multiplied by the quoted discount rate for that particular service category.
    e) SLAs as applicable will be deducted during the quarterly payment.

2.8 Appointment of Agency

Award Criteria

a) PESO/DPIITwill award the Contract to the successful MSP whose proposal has been determined to be substantially responsive and has been determined as the most responsive bids (“Best Value MSP”) as per the process outlined above.

Right to Accept Any Proposal and To Reject Any or All Proposal(s)

a) PESO/DPIITreserves the right to accept or reject any proposal, and to annul the tendering process / Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected MSP or MSPs or any obligation to inform the affected MSP or MSPs of the grounds of PESO/DPIIT action.

Notification of Award

a) Prior to the expiration of the validity period, PESO/DPIIT will notify the successful MSP in writing or email, that its proposal has been accepted. In case the tendering process / public procurement process has not been completed within the stipulated period, PESO/DPIIT may like to request the MSPs to extend the validity period of the bid.
b) The notification of award will constitute issue of a Letter of Intent (LoI) which needs to be acknowledged and signed by the successful MSP within 7 days from the date of issue of the letter. Upon the successful MSP's furnishing of Performance Guarantee, PESO/DPIIT will return the EMD of successful MSP.

2.9 Performance Guarantee

The PESO/DPIIT will require the selected MSP to provide a Performance Bank Guarantee, within 15 days from the Notification of award, for a value equivalent to 3% of the total cost of ownership (i.e. Contract value) followed by formation of contract. The Performance Guarantee should be valid for a period of 42 months (period of contract plus six months). The Performance Guarantee shall be kept valid till completion of the project in case of extension. The Performance Guarantee shall contain a claim period of three months from the last date of validity. The selected MSP shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period. In case the selected MSP fails to submit performance guarantee within the time stipulated, the PESO/DPIIT at its discretion may cancel the order placed on the selected MSP without giving any notice. PESO/DPIIT shall invoke the performance guarantee in case the selected agency fails to discharge their contractual obligations during the period or PESO/DPIIT incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions. The format for Performance Bank Guarantee is as provided at Annexure.

2.10 Signing of Contract

a) Post submission of Performance Guarantee by the successful MSP, PESO/DPIIT shall enter into a contract with the successful MSP incorporating all clauses, pre-bid clarifications and the proposal of the MSP.

2.10.1 Conditions for Contract

i. The contract duration is for 13 Months from the date of contract award as mentioned in the work order. Further to this, as per the user's requirement and with the consent of all stakeholders, the contract may be extended upon mutual agreement, for continuation of smooth services.

ii. Payment will be made on the basis of actual usage of the services. The period for which services will not be availed, shall not be paid.

iii. The incidental expenses of execution of agreement/contract shall be borne by the selected agency. The MSP will provide services as per PESO/DPIIT's requirements.

iv. The vendor should provide an escalation matrix for problem resolution to PESO/DPIIT by providing the Names, Designations, Contact Number(s) and Email ID's of the persons to be contacted. The agency should also provide website URL for such purpose. The selected agency must honor all tender conditions and adherence to all aspect of fair-trade practices in executing the purchase orders placed by PESO/DPIIT. Failing this, PESO/DPIIT may forfeit their PBG and stop further participation of such agency for three years in PESO/DPIIT tendering process.

v. In the event, the vendor company or the concerned division of the Company is taken over /bought over by another company, all the obligations and execution responsibilities under the agreement with PESO/DPIIT, should be passed on for compliance by the new company in the negotiation for their transfer.

vi. At any time, during the contract period, PESO/DPIIT may ask the agency to submit the supporting documents which may be required to ensure that the tender terms and conditions are fulfilled.

vii. The agency should not assign or sublet the work or any part of it to any other agency. Any such attempt shall result in termination of contract and forfeiture of the PBG.

viii. PESO/DPIIT may, at any time, terminate the contract by giving written notice to the vendor without any compensation, if the vendor becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to PESO/DPIIT.

ix. On getting written communication from PESO/DPIIT for having qualified for award of contract, the MSP shall provide acceptance and sign the contract within 7 days of such communication. Failing which the offer shall be treated as withdrawn.

x. After selection procedure for issuance of Work Order / Purchase Order will be at the sole discretion of PESO/DPIIT. The MSP will provide services as per PESO/DPIIT requirements.

xi. During the contract, PESO/DPIIT may ask the agency to submit the supporting documents which may be required to ensure that the tender terms and conditions are fulfilled.

xii. PESO/DPIIT reserves the right to utilize the discovered prices of the CSP services for any additional workload of PESO/DPIIT, applicable across various missions and departments with no price increase subject to commercial contract terms.

xiii. The selected agency should not assign or sublet the contract or any part of it to any other agency in any form. Any such attempt shall result in termination of contract and forfeiture of the security deposit, revocation of bank guarantees (including the ones submitted for other work orders)

xiv. Reasons for rejecting a tender/bid will be disclosed to a MSP only where enquiries are made.

2.11 Exit Management and Knowledge Transfer

Exit Management

The selected MSP shall prepare an Exit Management Plan for transfer of operations to PESO/DPIIT and/or as may be advised by PESO/DPIIT in the event of termination or expiry of the contract with PESO/DPIIT, without affecting services to stakeholders adversely. All the below mentioned responsibilities of MSP (from **MEITY guidelines on Cloud Services**) need to be followed:

i. Assist the PESO/DPIIT in migrating the VMs, data etc, whenever required.

ii. Migration of the VMs, data, content and any other assets to the new environment and ensuring successful deployment and running of the Government Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Department supplied industry standard media.

iii. The format of the data transmitted from the CSP to the Department should leverage standard data formats (e.g., OVF, VHD...) whenever possible to ease and enhance portability.

iv. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with PESO/DPIIT.

v. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date

vi. Ensure that the CSP does not delete any data at the end of the contract without the express approval of the PESO/DPIIT.

vii. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, content and data of the PESO/DPIIT as per stipulations and shall ensure that the data cannot be forensically recovered.

viii. Carry out the migration of the VMs, data, content and any other assets to the new environment created by the Government Department / Agency or any other Agency (on behalf of the Department) on alternate CSP's offerings to enable successful deployment and running of the PESO/DPIIT solution on the new infrastructure.

ix. Address and rectify the problems with respect to migration of the PESO/DPIIT application and related IT infrastructure during the transition.

x. Ensure that all the documentation required by the PESO/DPIIT for smooth

transition (in addition to the documentation provided by the CSP) are kept up to date and all such documentation is handed over to the PESO/DPIIT during regular intervals as well as during the exit management process.

xi. Support and assist the PESO/DPIIT for entire transition period so that l the PESO/DPIIT is able to successfully deploy and access the services from the new environment.

xii. Train and transfer the knowledge to the Replacement Agency (or PESO/DPIIT) to ensure similar continuity and performance of the Services post expiry of the contract.

The selected MSP shall get this process approved by PESO/DPIIT. The Plan shall include, but not be limited to, the following: -

a) Detailed Program of the Transfer Process that could be used in conjunction with a Replacement Agency 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.

b) Plans for the communication with such of PESO/DPIIT staff, OEM's and any related third party as are necessary to avoid any material detrimental impact on PESO/DPIIT project operations as a result of undertaking the transfer.

c) Plans for provision of contingent support to PESO/DPIIT and Replacement Agency for a reasonable period as mutually agreed with PESO/DPIIT.

d) The selected MSP shall draft the Exit Management Plan periodically thereafter to ensure that it is kept relevant and up to date.

e) Exit Management Plan shall be presented by the selected MSP to PESO/DPIIT and approved by PESO/DPIIT.

f) The Terms of Payment as stated in the Payment Schedule shall include the costs of the Agency complying with its obligations under Exit Plan.

g) During the Exit Management Period, the selected MSP shall use its best efforts to deliver the services.

h) The Exit Management plan shall be furnished in writing to PESO/DPIIT within ninety (90) days from the Effective Date of this Agreement.

i) The selected MSP shall be entitled to use the Assets for the duration of the exit management period

j) Promptly on reasonable request by PESO/DPIIT the MSP shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (provided by the MSP). PESO/DPIIT shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The selected MSP shall permit PESO/DPIIT or its nominated agencies to have reasonable access to its employees and facilities as reasonably required by PESO/DPIIT or PESO/DPIIT project management unit to understand the methods of delivery of the services employed by the MSP and to assist appropriate knowledge transfer.

k) Before the expiry of the exit management period, unless otherwise provided under the Contract, PESO/DPIIT or its nominated agency shall deliver to the MSP all forms of

MSP confidential information, which if any is in the possession or control of PESO/DPIIT, or its users.

l) Upon completion of the contract period or upon termination of the agreement for any reasons, the selected MSP shall comply with the following:

1. Notify to PESO/DPIIT forthwith the particulars of all Project Assets.
2. Deliver forthwith actual or constructive possession of the Project free and clear of all encumbrances and execute such deeds, writings and documents as may be required by PESO/DPIIT, for fully and effectively divesting the selected MSP of all of the rights, title and interest of the selected MSP in the Project and conveying the Project.

Knowledge Transfer

Knowledge Transfer is an integral part of the scope of work of the selected MSP. This will have to be done even in case the Contract with the selected MSP ends or is terminated before the planned timelines. The transition period shall span a minimum of one month or as mutually agreed with PESO/DPIIT. The selected MSP shall ensure during the exit management the following:

a. Handover all the deliverables and documents to the selected entity or resources as finalized by PESO/DPIIT.

b. Have a month of overlap period of running the operations with the MSP or as mutually decided between the selected MSP and PESO/DPIIT.

At the end of the Contract, the selected MSP will be required to provide necessary handholding and transition support to the designated staff or any other Agency that is selected for providing PMU services post the Contract with the selected MSP.

2.11 Failure to Agree with the Terms and Conditions of the RFP

a) Failure of the successful MSP to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event PESO/DPIIT may award the contract to the next best value MSP or call for new proposals from the interested MSPs, at its sole discretion.
b) In such a case, the PESO/DPIIT shall invoke the EMD of the most responsive MSP.

2.11.1 Fraud and Corrupt Practices

a) The Applicants/MSPs and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, the PESO/DPIIT shall reject a Proposal without being liable in any manner whatsoever to the Applicant, if it determines that the MSP has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the Selection Process. In such an event, the PESO/DPIIT shall, without prejudice to its any other rights or remedies, forfeit and appropriate the EMD or PBG, as the case may be, as mutually agreed genuine pre-estimated compensation and damages payable to the PESO/DPIIT for, inter alia, time, cost and effort of the PESO/DPIIT, in regard to the RFP, including consideration and evaluation of such Applicant's Proposal.

b) Without prejudice to the rights of the PESO/DPIIT under Clause above and the rights and remedies which the PESO/DPIIT may have under the Letter of Intent (LOI) or the Agreement, if an Applicant, as the case may be, is found by the PESO/DPIIT to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive

practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Agreement, such Applicant shall not be eligible to participate in any tender or RFP issued by the PESO/DPIIT during a period of 36 months from the date such Applicant, as the case may be, is found by the PESO/DPIIT to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

c) For the purposes of this Section, the following terms shall have the meaning hereinafter respectively assigned to them:

   i. "corrupt practice" means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the PESO/DPIIT who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the PESO/DPIIT shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the Letter of Intent (LOI) or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of the PESO/DPIIT in relation to any matter concerning the Project;

   ii. "Fraudulent practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process.

   iii. "Coercive practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the Selection Process;

   iv. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by PESO/DPIIT with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and

   v. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Applicants with the objective of restricting or manipulating a full and fair competition in the Selection Process.

2.11.2 Conflict of Interest

a) The Applicant shall warrant that, to the best of its knowledge after making diligent inquiry, at the time of submission of proposal that no conflict of interest exists or is likely to arise in the performance of its obligations under this RFP.

b) An Applicant shall not have a conflict of interest that may affect the Selection Process, or the work envisaged under this RFP (the "**Conflict of Interest**"). Any Applicant found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the PESO/DPIIT shall forfeit and appropriate the EMD, if available, as mutually agreed genuine pre-estimated compensation and damages payable to the PESO/DPIIT for, *inter alia*, the time, cost and effort of the PESO/DPIIT including consideration of such Applicant's Proposal, without

prejudice to any other right or remedy that may be available to the PESO/DPIIT hereunder or otherwise.

c) In the event that a MSP identifies a potential conflict of interest, they shall make a written disclosure to the PESO/DPIIT as soon as any potential conflict comes to their notice but in no case later than 7 (seven) days from the receipt of such proposals and any breach of this obligation of disclosure shall be construed as Conflict of Interest. The PESO/DPIIT shall, upon being notified by the agency under this Clause, decide and convey its decision to the agency within a period not exceeding 15 (fifteen) days.

d) Any breach in this specific conflict of interest clause will attract severe action, including but not limited to termination of contract and blacklisting.

2.12 Resolution of Disputes

a) Amicable settlement

The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Agreement or the interpretation thereof.

b) Dispute resolution

(i) Any dispute, difference or controversy of whatever nature howsoever arising under or out of or in relation to this Agreement (including its interpretation) between the Parties and so notified in writing by either Party to the other Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure set forth in Clause c.

(ii) The Parties agree to use their best efforts for resolving all Disputes arising under or in respect of this Agreement promptly, equitably and in good faith, and further agree to provide each other with reasonable access during normal business hours to all non-privileged records, information and data pertaining to any Dispute.

c) Conciliation

In the event of any dispute between the Parties, either Party may call upon PESO/DPIIT for amicable settlement, and upon such reference, the said persons shall meet no later than 10 (ten) days from the date of reference to discuss and attempt to amicably resolve the Dispute. If such meeting does not take place within the 10 (ten) day period or the Dispute is not amicably settled within 15 (fifteen) days of the meeting or the Dispute is not resolved as evidenced by the signing of written terms of settlement within 30 (thirty) days of the notice in writing referred to in Clause 3.8 b (i) or such longer period as may be mutually agreed by the Parties, either Party may refer the Dispute to arbitration in accordance with the provisions of Clause d.

d) Arbitration

i. Any Dispute which is not resolved amicably by conciliation, as provided in Clause c, shall be finally decided by reference to arbitration by an Arbitral Tribunal appointed in accordance with Clause d (ii) Such arbitration shall be held in accordance with the Rules of Arbitration of the International Centre for Alternative Dispute Resolution, New Delhi (the "Rules"), or such other rules as may be mutually agreed by the Parties, and shall be subject to the provisions of the Arbitration and Conciliation Act,1996 or any modifications, rules or re-enactments thereof. The place of such arbitration shall be Delhi and the language of arbitration proceedings shall be English.

ii. There shall be [a sole arbitrator whose appointment] / [an Arbitral Tribunal of three arbitrators, of whom each Party shall select one, and the third arbitrator shall be appointed by the two arbitrators so selected, and in the event of disagreement between the two arbitrators, the appointment] shall be made in accordance with the Rules.

iii. The arbitrators shall make a reasoned award (the "Award"). Any Award made in any arbitration held pursuant to Clause "Resolution of Disputes" shall be final and binding on the Parties as from the date it is made, and the Agency and the Authority agree and undertake to carry out such Award without delay.

iv. The Agency and the Authority agree that an Award may be enforced against the Agency and/or the Authority, as the case may be, and their respective assets wherever situated.

v. This Agreement and the rights and obligations of the Parties shall remain in full force and effect, pending the Award in any arbitration proceedings hereunder.

2.12.1 Liquidated Damages (LD) and Service Levels (SLAs) Penalty

Liquidated Damages for error/variation
In case any error or variation is detected in the reports submitted by the MSP and such error or variation is the result of negligence or lack of due diligence on the part of MSP, the consequential damages thereof shall be quantified in a reasonable manner and recovered from the MSP by way of deemed liquidated damages, subject to a maximum of 20% (Twenty per cent) of the cumulative billing of cloud services including MSP charges. If at any point MSP reaches to the maximum capped penalty amount, then contract may be terminated and deposited PBG can be forfeited.

Service Levels (SLAs) and Penalties (excluding 3rd party OEM products).

Sr. No	Service Level Objective/Criteria	Definition	Target	Penalty
Initial Setup				
1	Delay in Account setup and Readiness	Delay in Account setup, provisioning of initial requirement	7 days from the issuance of LOI	Within 7 days - Nil 1% of the total cost of the bid for every week's delay. If delay is more than 2 weeks, contract may be terminated.
Migration				
2	Successful Completion of Migration and Go-Live of all the mentioned applications and current PESO IT infrastructure as per the stipulated timeline with zero data loss and max 60 mins Downtime.	Migration completion will be considered successful, based on signed acceptance from PESO/DPIIT. This signed acceptance should be completed in the stipulated timeline.	Timeline as defined in the RFP SoW Within 45 days	5% of the total cost of the bid for every week's delay capped to maximum of 20% of the total cost of the bid. If delay is more than 4 weeks, contract may be terminated and PBG forfeited.
Availability				

3	Availability of each deployed cloud service (Applicable for all Cloud Service as defined in scope of work and BOM)	Availability means, the aggregate number of hours in a calendar month during which cloud service is available for use through command line interface, user/admin portal and APIs Uptime Calculation for the calendar month is as below: {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x100}	Availability for each of the cloud service>=99.5%	Penalty as indicated below (per occurrence): a) <99.5% to >= 99.00% - 10% of Monthly Payment of the Project b) <99.00% to >= 98.50% - 15% of Monthly Payment of the Project c) <98.50% - 20% of Monthly Payment of the Project In case the services are not available (through DC) for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the Monthly Payment of the Project.
Performance				

4	Provisioning of new Virtual Machine and/or container and/or other services (GPU, Storage, Managed DBs etc.)	Time to provision new Virtual Machine. Measurement shall be done by analysing the log files.	within 15 minutes	Penalty as indicated below (per occurrence): Within 15 minutes no penalty More than 15 minutes - 5% of the Monthly Payment of that Service
5	Spinning up the Object Storage	Time to spin up Object Storage. Measurement shall be done by analyzing the log files.	within 15 minutes	Penalty as indicated below (per occurrence): Within 15 minutes no penalty More than 15 minutes - 5% of the Monthly Payment of that Service
6	Response Time under Enterprise support	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	within 15 minutes	Penalty as indicated below (per occurrence): Within 15 minutes no penalty More than 15 Minute - 5% of the Monthly Payment of that Service

7	Wrong billing for services consumed	If overbilling is done, the penalty = over bill - bill after correction	NA	100% amount on difference of actual bill and wrong bill to be paid
Service levels for Disaster Recovery				
8	Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO is as per declaration provided by MSP/CSP	0.5% of total cost of the bid per every additional 1 (one) hours of downtime
9	Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO is as per declaration provided by MSP/CSP	0.5% of total cost of the bid per every additional 15 minutes of downtime

Note:

- MSP team should provide enterprise support at any time (24 hours a day, 7 days a week) via all possible modes including phone, chat, and email support to PESO/DPIIT team for provisioning and configuring cloud resources. They should be available at any given point of time for supporting the ongoing operation. The MSP cloud team leader will report to PESO/DPIIT Officer or coordinate with PMU team to update on the cloud operations and any other project or infrastructure related discussion.

2.13 Miscellaneous

The Selection Process shall be governed by, and construed in accordance with, the laws of India and the Courts at New Delhi shall have exclusive jurisdiction over all disputes arising under, pursuant to and/or in connection with the Selection Process.

2.13.1 The Client, in its sole discretion and without incurring any obligation or liability, reserves the right, at any time, to:

(i) suspend and/or cancel the Selection Process and/or amend and/or supplement the Selection Process or modify the dates or other terms and conditions relating thereto;

(ii) consult with any Applicant in order to receive clarification or further information;

(iii) retain any information and/or evidence submitted to the Client by, on behalf of and/or in relation to any Applicant; and/or

(iv) Independently verify, disqualify, reject and/or accept any and all submissions or other information and/or evidence submitted by or on behalf of any Applicant.

2.13.2 It shall be deemed that by submitting the Proposal, the Applicant agrees and releases the Client, its employees, agents and advisers, irrevocably, unconditionally, fully and finally from any and all liability for claims, losses, damages, costs, expenses or liabilities in any way related to or arising from the exercise of any rights and/or performance of any obligations

hereunder, pursuant hereto and/or in connection herewith and waives any and all rights and/ or claims it may have in this respect, whether actual or contingent, whether present or future.

2.13.3 All documents and other information provided by Client or submitted by an Applicant to Client shall remain or become the property of Client. Applicants and the Agency, as the case may be, are to treat all information as strictly confidential. Client will not return any Proposal or any information related thereto. All information collected, analyzed, processed or in whatever manner provided by the Applicant to Client in relation to the assignment shall be the property of Client.

2.13.4 The Client reserves the right to make inquiries with any of the clients listed by the Applicants in their previous experience record.

2.14 Tentative schedule for selection process

The Client will endeavour to follow the following schedule:

Date of issue of RFP	11th September 2026
Last date for receiving queries/requests for clarification	15th September 2026 upto 11:00 AM
Pre-bid meeting	15th September 2026 at 3:00 PM (via vc)
Client's response to queries/requests for clarification	21st September 2026
Last date of submission of Bids/Submission EMD	24th September 2026 by 4:00 PM
Date of opening of technical Bids	25th September 2026 by 12:00 PM
Opening of financial Bid	To be informed later

*Applicant may note that the venue and time of opening of financial bid shall be posted on official website of client after presentation by applicants.

In addition to Certificates/Receipts/Statements/Letters/ Documents, etc., as prescribed in this RFP, the following standard forms are required for pre-qualification and technical proposal.

Form 3A	Pre – Qualification Proposal Submission Form
Form 3B	Format for Power of Attorney for Authorized representative
Form 3C	Format of Bank Guarantee for Earnest Money Deposit
Form 3D	Technical Proposal Submission
Form 3E	Profile of Agency/ Institution

*Please attach a clear scan copy of all the documents

Form 3A: Pre-Qualification Proposal Submission Form

[Location, Date]

To

O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in

RFP dated (date) for selection of Agency for [name of assignment]

Dear Sir,

With reference to your RFP Document dated [date], we, having examined all relevant documents and understood their contents, hereby submit our Pre-Qualification Proposal for selection as [name of assignment]. The Proposal is unconditional and unqualified.

We are submitting our Proposal as [name of the Applicant].

We understand you are not bound to accept any Proposal you receive. Further:

1. We acknowledge that Client will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Agency, and we certify that all information provided in the Proposal and in the supporting documents is true and correct, nothing has been omitted which renders such information misleading; and all documents accompanying such Proposal are true copies of their respective originals.

1. This statement is made for the express purpose of appointment as the Agency for the aforesaid Project.
2. We shall make available to Client any additional information it may deem necessary or require for supplementing or authenticating the Proposal.
3. We acknowledge the right of Client to reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any account whatsoever.
4. We certify that in the last 3 (three) years, we have neither failed to perform on any assignment or contract, as evidenced by imposition of a penalty by an arbitral or judicial authority or a judicial

pronouncement or arbitration award against the Applicant, nor been expelled from any project, assignment or contract by any public authority nor have had any assignment or contract terminated by any public authority for breach on our part.

5. We declare that:

a. We have examined and have no reservations to the RFP, including any Addendum issued by the Authority;

b. We do not have any conflict of interest in accordance with the terms of the RFP;

c. We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as defined in the RFP document, in respect of any tender or request for proposal issued by or any agreement entered into with Client or any other public sector enterprise or any government, Central or State; and

d. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

7. We understand that you may cancel the selection process at any time and that you are neither bound to accept any Proposal that you may receive nor to select the Agency, without incurring any liability to the Applicants.

8. We declare that we are not a member of any other Consortium/JV applying for selection as an Agency.

9. We certify that in regard to matters other than security and integrity of the country, we or any of our affiliates have not been convicted by a court of law or indicted or adverse orders passed by a regulatory authority which would cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.

10. We further certify that in regard to matters relating to security and integrity of the country, we have not been charge-sheeted by any agency of the Government or convicted by a court of law for any offence committed by us or by any of our affiliates. We further certify that neither we nor any of our consortium members have been barred by the central government, any State Government, a statutory body or any public sector undertaking, as the case may be, from participating in any project or bid, and that any such bar, if any, does not subsist as on the date of this RFP.

11. We further certify that no investigation by a regulatory authority is pending either against us or against our affiliates or against our CEO or any of our Directors/ Managers/ employees.

12. We hereby irrevocably waive any right or remedy which we may have at any stage at law or howsoever otherwise arising to challenge or question any decision taken by Client in connection with the selection of Agency or in connection with the selection process itself in respect of the above-mentioned Project.

13. We agree and understand that the proposal is subject to the provisions of the RFP document. In no case, shall we have any claim or right of whatsoever nature if the Project is not awarded to us or our proposal is not opened or rejected.

14. We agree to keep this offer valid for 60 (sixty) days from the POD specified in the RFP.

15. A Power of Attorney in Favor of the authorized signatory to sign and submit this Proposal and documents is attached herewith.

16. The Technical and Financial Proposal is being submitted in a separate cover. This Pre Qualification Proposal read with the Technical and Financial Proposal shall constitute the application which shall be binding on us.

We agree and undertake to abide by all the terms and conditions of the RFP Document.

We remain,

Yours sincerely,

Authorized signature Name and title of signatory Name of Firm

Address:

Telephone:

Fax:

(Name and seal of the Applicant/Member in Charges)

Form 3B: Format for Power of Attorney for Authorized Representative

Know all men by these presents, We, [name of organization and address of the registered office] do hereby constitute, nominate, appoint and authorize Mr./Ms. [name], son/ daughter/ wife of [name], and presently residing at [address], who is presently employed with/ retained by us and holding the position of [designation] as our true and lawful attorney (hereinafter referred to as the –Authorized Representative), with power to sub- delegate to any person, to do in our name and on our behalf, all such acts, deeds and things as are necessary or required in connection with or incidental to submission of our Proposal for and selection as Agency for [name of assignment], to be developed by PESO/DPIIT (the –Authority) including but not limited to signing and submission of all applications, proposals and other documents and writings, participating in pre-bid and other conferences and providing information/ responses to the Authority, representing us in all matters before the Authority and undertakings consequent to acceptance of our proposal and generally dealing with the Authority in all matters in connection with or relating to or arising out of our Proposal for the said Project and/or upon award thereof to us until accepting the work order with the Authority.

AND, we do hereby agree to ratify and confirm all acts, deeds and things lawfully done or caused to be done by our said Authorized Representative pursuant to and in exercise of the powers conferred by this Power of Attorney and that all acts, deeds and things done by our said Authorized Representative in exercise of the powers hereby conferred shall and shall always be deemed to have been done by us.

IN WITNESS WHEREOF WE, [name of organization], THE ABOVE-NAMED PRINCIPAL HAVE

EXECUTED THIS POWER OF ATTORNEY ON THIS [date in words] DAY OF [month] [year in yyyy format].

For [name and registered address of organization] [Signature] [Name]

[Designation] Witnesses:

1. [Signature, name and address of witness]
2. [Signature, name and address of Witness] Accepted

Signature] [Name] [Designation] [Address] Not

Note:

1. The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under seal affixed in accordance with the required procedure.

2. Wherever required, the Applicant should submit for verification the extract of the charter documents and other documents such as a resolution/power of attorney in Favor of the person executing this Power of Attorney for the delegation of power hereunder on behalf of the Applicant.

3. For a Power of Attorney executed and issued overseas, the document will also have to be legalized by the Indian Embassy and notarized in the jurisdiction where the Power of Attorney is being issued. However, the Power of Attorney provided by Applicants from countries that have signed The Hague Legislation Convention, 1961 are not required to be legalized by the Indian Embassy if it carries a conforming Apostille certificate.

Form 3C: Format of bank Guarantee for Earnest Money Deposit

BG No.

Date:

1. In consideration of you O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in (hereinafter referred to as the –Authority which expression shall, unless repugnant to the context or meaning thereof, include its administrators, successors and assigns) having agreed to receive the proposal of **[Name of company],** (hereinafter referred to as the –Bidder which expression shall unless it be repugnant to the subject or context thereof include its successors and assigns), for appointment as Agency for [name of assignment] pursuant to the RFP Document dated [date] issued in respect of the Assignment and other related documents including without limitation the draft work order for services (hereinafter collectively referred to as –RFP Documents), we [Name of the Bank] having our registered office at [registered address] and one of its branches at [branch address] (hereinafter referred to as the –Bank), at the request of the Bidder, do hereby in terms of relevant clause of the RFP Document, irrevocably, unconditionally and without reservation guarantee the due and faithful fulfillment and compliance of the terms and conditions of the RFP Document by the said Bidder and unconditionally and irrevocably undertake to pay forthwith to the Authority an amount of Rs. [in figures] ([in words]) (hereinafter referred to as the –Guarantee) as our primary obligation without any demur, reservation, recourse, contest or protest and without reference to the Bidder if the Bidder shall fail to fulfill or comply with all or any of the terms and conditions contained in the said RFP Document.

2. Any such written demand made by the Authority stating that the Bidder is in default of the due and faithful fulfillment and compliance with the terms and conditions contained in the RFP Document shall be final, conclusive and binding on the Bank. We, the Bank, further agree that the Authority shall be the sole judge to decide as to whether the Bidder is in default of due and faithful fulfillment and compliance with the terms and conditions contained in the RFP Document including, Document including without limitation, failure of the said Bidder to keep its Proposal valid during the validity period of the Proposal as set forth in the said RFP Document, and the decision of the Authority that the Bidder is in default as aforesaid shall be final and binding on us, notwithstanding any differences between the Authority and the Bidder or any dispute pending before any court, tribunal, arbitrator or any other authority.

3. We, the Bank, do hereby unconditionally undertake to pay the amounts due and payable under this Guarantee without any demur, reservation, recourse, contest or protest and without any reference to the Bidder or any other person and irrespective of whether the claim of the Authority is disputed by the Bidder or not, merely on the first demand from the Authority stating that the amount claimed is due to the Authority by reason of failure of the Bidder to fulfil and comply with the terms and conditions contained in the RFP Document including without limitation, failure of the said Bidder

to keep its Proposal valid during the validity period of the Proposal as set forth in the said RFP Document for any reason whatsoever. Any such demand made on the Bank shall be conclusive as regards amount due and payable by the Bank under this Guarantee. However, our liability under this Guarantee shall be restricted to an amount not exceeding Rs. [in figures] ([in words]).

4. This Guarantee shall be irrevocable and remain in full force for a period of 60(sixty) days from the Proposal Due Date and a further claim period of thirty (30) days or for such extended period as may be mutually agreed between the Authority and the Bidder, and agreed to by the Bank, and shall continue to be enforceable until all amounts under this Guarantee have been paid.

5. The Guarantee shall not be affected by any change in the constitution or winding up of the Bidder or the Bank or any absorption, merger or amalgamation of the Bidder or the Bank with any other person.

6. In order to give full effect to this Guarantee, the Authority shall be entitled to treat the Bank as the principal debtor. The Authority shall have the fullest liberty without affecting in any way the liability of the Bank under this Guarantee from time to time to vary any of the terms and conditions contained in the said RFP Document or to extend time for submission of the Proposals or the Proposal validity period or the period for conveying of Letter of Acceptance to the Bidder or the period for fulfilment and compliance with all or any of the terms and conditions contained in the said RFP Document by the said Bidder or to postpone for any time and from time to time any of the powers exercisable by it against the said Bidder and either to enforce or forbear from enforcing any of the terms and conditions contained in the said RFP Document or the securities available to the Authority, and the Bank shall not be released from its liability under these presents by any exercise by the Authority of the liberty with reference to the matters aforesaid or by reason of time being given to the said Bidder or any other forbearance, act or omission on the part of the Authority or any indulgence by the Authority to the said Bidder or by any change in the constitution of the Authority or its absorption, merger or amalgamation with any other person or any other matter or thing whatsoever which under the law relating to sureties would but for this provision have the effect of releasing the Bank from its such liability.

7. Any notice by way of request, demand or otherwise hereunder shall be sufficiently given or made if addressed to the Bank and sent by courier or by registered mail to the Bank at the address set forth herein.

8. We undertake to make the payment on receipt of your notice of claim on us addressed to (Name of bank along with branch address] and delivered at our above branch which shall be deemed to have been duly authorized to receive the said notice of claim.

9. It shall not be necessary for the Authority to proceed against the said Bidder before proceeding against the Bank and the guarantee herein contained shall be enforceable against the Bank, notwithstanding any other security which the Authority may have obtained from the said Bidder or any other person and which shall, at the time when proceedings are taken against the Bank hereunder, be outstanding or unrealized.

10. We, the Bank, further undertake not to revoke this Guarantee during its currency except with the previous express consent of the Authority in writing.

11. The Bank declares that it has power to issue this Guarantee and discharge the obligations contemplated herein, the undersigned is duly authorized and has full power to execute this Guarantee for and on behalf of the Bank.

12. For the avoidance of doubt, the Bank's liability under this Guarantee shall be restricted to Rs. [in figures] ([in words]). The Bank shall be liable to pay the said amount or any part thereof only if the Authority serves a written claim on the Bank in accordance with paragraph 8 hereof, on or before [date].Signed and Delivered by [name of bank]

By the hand of Mr. /Ms. [name], it's (designation] and authorized official.

(Signature of the Authorized Signatory) (Official Seal)

Notes:

The Bank Guarantee should contain the name, designation and code number of the officer(s) signing the Guarantee.

The address, telephone number and other details of the Head Office of the Bank as well as of issuing Branch should be mentioned on the covering letter of issuing Branch

Form 3D: Technical Proposal Submission Form

[Location, Date]

O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440006 | Seminary Hills, Nagpur Maharashtra – 440006 Email: explosives@explosives.gov.in

RFP dated [date] for selection for [name of assignment]

Sir,

With reference to your RFP Document dated [date], we, having examined all relevant documents and understood their contents, hereby submit our Technical Proposal for selection as [name of assignment]. The Proposal is unconditional and unqualified.

We are submitting our Proposal as [name of the applicant].

If negotiations are held during the period of validity of the Proposal, we undertake to negotiate in accordance with the RFP. Our Proposal is binding upon us, subject only to the modifications resulting from negotiations in accordance with the RFP.

We understand you are not bound to accept any Proposal you receive. Further:

1. We acknowledge that Client will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Agency, and we certify that all information provided in the Proposal and in the supporting documents is true and correct, nothing has been omitted which renders such information misleading; and all documents accompanying such Proposal are true copies of their respective originals.

2. This statement is made for the express purpose of appointment as the Agency for the aforesaid Project.

3. We shall make available to Client any additional information it may deem necessary or require for supplementing or authenticating the Proposal.

4. We acknowledge the right of Client to reject our application without assigning any reason or otherwise and hereby waive our right to challenge the same on any account whatsoever.

5. We certify that in the last 3 (three) years, we have neither failed to perform on any assignment or contract, as evidenced by imposition of a penalty by an arbitral or judicial authority or a judicial pronouncement or arbitration award against the Applicant, nor been expelled from any project, assignment or contract by any public authority nor have had any assignment or contract terminated by any public authority for breach on our part.

6. We declare that:-
    a. We have examined and have no reservations to the RFP, including any Addendum issued by the Authority;
    b. We do not have any conflict of interest in accordance with the terms of the RFP;

c. We have not directly or indirectly or through an agent engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as defined in the RFP document, in respect of any tender or request for proposal issued by or any agreement entered into with Client or any other public sector enterprise or any government, Central or State; and
d. We hereby certify that we have taken steps to ensure that no person acting for us or on our behalf will engage in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

7. We understand that you may cancel the selection process at any time and that you are neither bound to accept any Proposal that you may receive nor to select the Agency, without incurring any liability to the Applicants.

8. We certify that in regard to matters other than security and integrity of the country, we or any of our affiliates have not been convicted by a court of law or indicted or adverse orders passed by a regulatory authority which would cast a doubt on our ability to undertake the Project or which relates to a grave offence that outrages the moral sense of the community.

9. We further certify that in regard to matters relating to security and integrity of the country, we have not been charge-sheeted by any agency of the Government or convicted by a court of law for any offence committed by us or by any of our affiliates. We further certify that neither we nor any of our consortium members have been barred by the central government, any state government, a statutory body or any public sector undertaking, as the case may be, from participating in any project or bid, and that any such bar, if any, does not subsist as on the date of this RFP.

10. We further certify that no investigation by a regulatory authority is pending either against us or against our affiliates or against our CEO or any of our Directors/ Managers/ employees.

11. We hereby irrevocably waive any right or remedy which we may have at any stage at law or howsoever otherwise arising to challenge or question any decision taken by Client in connection with the selection of Agency or in connection with the selection process itself in respect of the above-mentioned Project.

12. We agree and understand that the proposal is subject to the provisions of the RFP document. In no case, shall we have any claim or right of whatsoever nature if the Project is not awarded to us or our proposal is not opened or rejected.

13. The Financial Proposal is being submitted in a separate cover. This Technical Proposal read with the Financial Proposal shall be binding on us.

14. We agree and undertake to abide by all the terms and conditions of the RFP Document.

We remain, yours sincerely,

Authorized Signature [In full and initials]: Name and Title of Signatory:

Name of Firm:

Address:

Telephone:

Fax:

(Name and seal of the Applicant/Member in Charge)

Form 3E: Profile of Agency/ Institution

{Location, Date]

— Brief Profile of Applicant (in one page)

— Number of offices with locations in India

— Global presence

4. Section 4. Financial Proposal – Standard Forms

Form 4A: Financial Proposal Submission

Form 4B: Summary of Costs

Form 4A: Financial Proposal Submission Form

[Location] [Date]

O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-

Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email:

explosives@explosives.gov.in

Dear Sir

Subject: Services for [name of assignment].

We, the undersigned, offer to provide the services for [name of assignment] in accordance with your Request for Proposal dated [date] and our Proposal. Our attached Financial Proposal is for the sum of [amount(s) in words and figures) (including GST)

Our Financial Proposal shall be binding upon us subject to the modifications resulting from arithmetic correction, if any, up to expiration of the validity period of the Proposal, i.e. [date].

We undertake that, in competing for (and, if the award is made to us, in executing) the above assignment, we will strictly observe the laws against fraud and corruption in force in India namely – Prevention of Corruption Act 1988.

We understand you are not bound to accept any Proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: Name and Title of Signatory:

Name of Firm:

Address:

Form 4B: Summary of Costs

Sr.	Cost Head (A)	Cost (Recurring) (B) (INR)	MSP Discount in (%) (C)	Bid Price for 13 months in INR (D)
1	CSP Usage Cost per Month, including Enterprise support cost as per BoM (Refer Annexure C)	₹0.00		₹0.00
2	Manpower Charges for Migration services		Not applicable	₹0.00
3	Per unit Hourly cost of CSP Professional Services to be taken as per requirement (on-demand basis) - 24 Hours per month		Not Applicable	₹0.00
4	Managed Service Provider Cost for Manpower for Maintenance and management of Cloud infrastructure - in percentage of Monthly CSP Usage Cost		Not Applicable	₹0.00
5	Cost of 3rd Party Security components including installation and commissioning - Lumpsum`(Refer Annexure D)	₹0.00	Not Applicable	₹0.00
6	Training and Capacity Building - Lumpsum		Not Applicable	₹0.00
TOTAL PRICE				**₹0.00**
Taxes - GST@18%				**₹0.00**
TOTAL BID PRICE				**₹0.00**
TOTAL BID PRICE (IN WORDS)				

Additional Notes

1. The bid value shall include all taxes and levies, including GST (Goods and Services Tax), and shall be in Indian Rupees (₹). Since, CSP public costing is in USD, MSP is required to quote price at conversion rate of 1USD=95 INR. For purpose of clarification, since publicly listed pricing of CSP is in USD, all payments will be made based on exchange rate (RBI) of the day of invoice generated. Bidder are not required to consider any cost associated with exchange rate fluctuation for financial bid.
2. In case service consumed in future by ministry is not listed in BoM or a variation of service is not listed in BoM, the payments shall be made based on actual invoice adjusted to above discount rate quoted by MSP under E5 cell
3. No cells in above table that are colored should be tampered with. All the cells with color are coded with formula or financial bid details.

Item	Amount in words	Amount in figures
Cost of Financial Proposal		
Goods and Services Tax (GST) should be inclusive of the amount proposed.		

****The payment shall be made based on payment terms in Clause 6.7***
#This value shall be the fee for the complete assignment (two years)

For Financial Evaluation, the total fee for the period will be considered. This Quoted Fee will cover costs/expenses of the Selected Agency for undertaking work as detailed in the Scope of Work. This financial proposal covers Stationary & IT equipment and out of pocket expenses for local travel in Delhi NCR. Expenses for outstation travel will be reimbursed to the selected agency. GST would be payable at the applicable rates as may be in force from time to time.

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

5. Scope of Work

PESO/DPIIT will be requiring a combination of all the 3 cloud deployment models, i.e – IaaS, PaaS and SaaS. The 3 models will be utilized across various service categories like compute, storage, networking & security - IaaS, containers & databases - PaaS and Analytics & Data warehousing – PaaS/SaaS. The PESO website is deployed on an Active-Active DC/DR Setup for High availability and near zero data loss (on physically separate Meity empanelled Data Centres) with Far DR for additional backup copy. The successful MSP is expected to provide a cloud environment that will aid in continuing with a similar highly available architecture with near zero data loss and a Far DR for backup. The other PSEO applications are currently deployed on-premises and need to be migrated to the proposed cloud. Additionally, the MSP shall have to perform the following activities as per the scope of work given below, but not limited to:

5.1 Migration of PESO applications

The selected MSP will be responsible for end-end successful migration of the existing PESO IT infrastructure.

Phase 1 - Migration

This phase shall comprise the following:

i. Complete understanding of the architecture of applications/projects
ii. Identification of all the components of the technology stack, their dependencies & integrations – both internal and external, configurations, keys and certificates, domain settings, security settings etc.
iii. Deployment of all the components of the stack on the MSP's proposed CSP's infrastructure in their respective environments (dev, staging, production etc.)
iv. Setup Open forge (Git repo of several projects), after its migration to the MSP's proposed cloud infra) for use by different applications for development and deployment (CI/CD).
v. Deployment and setup of all CI/CD pipeline.
vi. Any application development required as per new proposed services
vii. Performance and security benchmarks of the migrated projects/applications shall be same as that of the production deployment of the current ones. The MSP shall carry out load/performance testing and security testing and provide the report for this.
viii. Data transfer: The MSP shall provide all necessary support and tools for data transfer to the proposed CSP such as VPN tunnel for data transfer, data transfer tools etc. There shall be no additional cost implication for this and shall be covered under the Migration service.

Phase 2 – Go-Live

For the purpose of RFP, "Go-Live" is defined as the date on which all the projects/applications are completely operational in the production environment in a state (functionalities, performance, security etc.) same as the currently deployed ones and accepted by PESO.

a. The MSP shall prepare and agree with PESO on the detailed plan for Go-Live.
b. The MSP shall ensure that Go – Live criteria as mentioned in Go – Live plan is met.
c. A comprehensive system should be set up to perform load and security testing, log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified in Go-live of the application. The MSP shall be responsible for resolving all issues preventing Go-Live of all the projects. Post Go-Live, the Production environment should not be used for testing and training purposes. If any Production data is used for testing, it should be masked and it should be protected.

** The period for Migration and Go-Live is 45 days, post provisioning of required infrastructure. Please refer section "Delivery Schedule/Timelines".*

Phase 3 - Stabilization

The MSP shall be responsible for stabilization of the redeployed projects/applications. The Stabilization period is defined as the period during which the MSP has to do a parallel run of both the systems at on-premises/current CSP as well as the new selected CSP. The stabilization period will be for a period of 45 days after go-live to ensure success of the migration to the new CSP.

Other Conditions

i. During the migration period to the cloud, the MSP shall bring manpower with necessary technical experts to carry out the migration work. The resources should comprise of and not limited to - Delivery/Migration Manager, Cloud Solution Architect, Cloud Engineer, Cloud System Administrator, Cloud Database SME, Cloud Security Expert. Technical evaluation of the MSP shall include quality of these resources based on their interview and understanding of the projects. The MSP shall ensure that same resources are deployed in the migration process.
ii. The MSP shall be provided with all the necessary information, documentation and support from PESO resources. However, in absence of these also the MSP shall carry out the migration successfully without any dependency on these.
iii. The MSP shall be responsible for any Risk Management and Planning, or issues related to migration of data and mitigation of all the risks related to migration.
iv. MSP shall be responsible for security of resources, network infrastructure along with implementation of security compliances.
v. MSP shall be responsible for on-time completion of all the migration activities as defined in this RFP.
vi. MSP to provide a mechanism for the bulk transfer of all data, scripts, software, virtual machine images etc. as well as offline data transfer.
vii. Successful completion of migration shall mean completion of all the phases – Migration, Go-Live and Stabilization successfully.
viii. The MSP should ensure the following during the migration:
    a. Features and Capabilities of services during migration to be validated by the MSP's Cloud Professional Services team pre- and post-migration with the PESO project team.
    b. There should not be any downtime during migration activity (except as defined in the SLA).
    c. MSP needs to ensure no data loss during migration.
    d. MSP shall perform the end-to-end migration activities including quality checks, testing of environments as specified.
    e. Any Third-Party tool/ services required for migration, testing, benchmarking etc. is the responsibility of the MSP
    f. MSP shall be responsible for providing cloud training, certification etc. of PESO manpower for the proposed CSP in co-ordination with them
    g. The engagement of CSP engineers /solution architect or any Cloud Services Professional Cost (defined in the RFP) required during the Migration phase will be the responsibility of the MSP.
    h. The cost of rectification of non-compliances shall be borne by the MSP.

5.2 Cloud Services and Support

a. Setup the cloud account of the Cloud Service Provider (CSP) proposed in the bid: The MSP would be responsible for providing cloud for setting up, installation, configuration, management, up gradation, migration of application servers, database servers/storage, security etc. and also maintain and manage and configure the VMs, Containers, Storage, Network, Database etc.

b. The MSP shall be responsible to monitor the cloud services for all services. MSP will provide the support to PESO for Deployment of New Applications on cloud, security administration, planning and implementation of cloud management and monitoring portals for complete infrastructure and services procured and reporting services. The DevOps is also part of the application, in case of migration or use of any new service, support from MSP is required.
c. The MSP shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services. The MSP may provide documentation in globally accepted format/standards.
d. The MSP shall assist PESO in planning for capacity building to meet growth and peak load assessment from time to time, to ensure future requirements of PESO are addressed.
e. The MSP shall provide the relevant reports, including real time as well as past data/reports on dashboard.
f. MSP shall be responsible for conduct of Business Continuity and follow Standard Operating Procedures (SOP) and inform PESO in advance for such drills conducted twice a year normally, with 15 days' prior notice.
g. MSP will train and transfer the knowledge to the replacement agency or PESO to ensure continuity and performance of services post expiry of Contract
h. Provide report on utilization and optimization of the resources. PESO may review it on monthly basis.
i. Optimize the resources/manage services for optimum billing with satisfactory service.
j. Provide portal logins for billing, provisioning, usage etc. as per the requirement of the projects.
k. Provide Enterprise grade support at any time (24 hours a day, 7 days a week) via all possible modes including phone, chat, and email support to PESO and MSP for provisioning and configuring cloud resources.
l. The MSP will provide the real time dashboard for monitoring and financial aspects.

5.3 Cloud Service Provider Support

The CSP Professional team shall assist the MSP and the PESO/DPIIT team by providing inputs in the areas of solution architecture design and security aspects. The recommendations of the CSP would be binding to the MSP for compliance. They will also provide review inputs for scalability and desired functional and technical requirements and ensuring optimal utilization of cloud services and costs. The team will assist in the following:

a. Inputs for application design leveraging cloud native services: assist in building the application architecture, building the development and deployment pipeline, review of application architecture as per the best practices and provide a high-level solution architecture, migration plan and success metrics. Key activities and deliverables include:
    I. Assistance in building modernized application architecture based on micro services.
    II. Assistance in building development and deployment pipeline (CI/CD)
    III. Application Architecture Review regarding containerization, serverless, AI/ML, and analytics.
    IV. A high-level solution architecture, migration plan and success metrics
b. Security assessment of cloud resources: Assist in conducting a security assessment of cloud workloads. The assessment should comprehensively cover core security domains like Identity and Access Management, Infrastructure Security, Container Security, Data Protection, Visibility and Auditability Control and Incident Response capabilities. Based on the assessment, the CSP should provide a maturity assessment report against cloud security best practices and identify target based, prioritized findings and recommendations from improving the security posture. Key activities and deliverables include:

I. Detailed cloud security assessment to cover core security domains
II. Identification of target based, prioritized findings and recommendations for improving the cloud security posture
III. Maturity assessment report against cloud security best practices

c. Weekly, Monthly and Quarterly reviews (Security, Operation, Cost Optimization, Reliability, Performance, Sustainability) to be submitted to PESO by CSP professional services.
d. CSP and MSP are responsible of successful migration of different projects/applications to the proposed cloud. CSP and MSP will certify that the migration, to the new system has been done successfully and optimized to the best possible manner using services. In case of any discrepancy / delay/challenge during migration, CSP & MSP takes ownership to deploy professional services without any additional cost implications for successful migration of projects as defined in this RFP.

5.4 CSP Professional Services support

The MSP will also provide Professional Cloud Services from the CSP. The CSP cloud professional team shall also assist the MSP and the PESO team by providing inputs in the areas of solution architecture design and security aspects during the migration as well as throughout the contract period. The team will also provide review inputs for scalability and desired functional and technical requirements and ensure optimal utilization of cloud services and optimisation of cost. The team will assist in the following:

a. Inputs for application design leveraging cloud native services –assist in building the application architecture, building the development and deployment pipeline, review of application architecture as per the best practices and provide a high-level solution architecture, migration plan and success metrics.
b. Assistance in building modernized application architecture based on microservices.
   I. Assistance in building development and deployment pipeline (CI/CD)
   II. Application Architecture Review as per containerization, serverless, AI/ML, BigData processing, Data warehouse and analytics.
c. A high-level solution architecture, migration plan and success metrics, security assessment of cloud resources
d. Assist in conducting a security assessment of cloud workloads.
   I. The assessment should comprehensively cover core security domains like Identity and Access Management, Infrastructure Security, Container Security, Data Protection, Visibility and Auditability Control and Incident Response capabilities.
   II. Based on the assessment, the CSP should provide a maturity assessment report against cloud security best practices and identify target based, prioritized findings and recommendations from improving the security posture.
e. Key activities and deliverables include:
   I. Detailed cloud security assessment to cover core security domains
   II. Identification of target based, prioritized findings and recommendations for improving the cloud security posture
   III. Maturity assessment report against cloud security best practices
   IV. Weekly, Monthly and Quarterly reviews (Security, Operation, Cost Optimization, Reliability, Performance, and Sustainability) to be submitted to PESO by CSP professional services/MSP.

5.5 Change Request

This describes the procedure to be followed in the event of any proposed change to the scope of work and SLAs. Such change shall, inter alia, include:

- Requests for requirements changes (additions, deletions, modifications, deferrals) in Scope of Work (including software)
- Requests for resolving the problems in current production systems
- Requests for enhancements in current production systems d) Requests for new development projects.

The Change Control procedure applies to base-lined work products created or managed by the members of the PESO project. The Change Control process excludes any work products that are still under development or are a part of the scope of this RFP.

For evaluation of the financial cost of such change requests, a Change Advisory Board (CAB) shall be constituted by PESO with the following composition.

- PESO
- MSP
- Any agency nominated/engaged by PESO

The Chairperson of the Change Advisory Board (CAB) shall be PESO employee or PESO nominated individual. The final decision authority shall be the Chairperson.

On receiving any change request from CAB, the MSP shall submit its proposal with all the required information in a prescribed format for CAB's perusal. The prescribed format shall be specified by PESO.

CAB shall consider the change in context and come into action only when the change or any work is out of the scope of this RFP.

The CAB will examine the financial impact of the change and the charges for such a change will be decided based on the recommendation of CAB. The payment for such changes will be as per the Terms of Payment to be decided by PESO.

Disaster Recovery

- MSP is required to perform disaster recovery test to determine successful configuration of DR plan at determined RPO/RTO. For the purpose, MSP is required to support department to conduct DR drills for the application.
- MSP is required to demonstrate ability of cloud services to be available during the drills as per determined RPO/RTO.
- MSP is required to maintain synchronous replication of data between Primary DC and NDR and asynchronous between DC and Far DR. MSP shall propose Active-Active architecture for the data replication between DC and, NDR & Active-Passive for DC and Far-DR. All data centers have to be Meity empaneled.
- MSP/CSP will be responsible for sizing of the compute & other cloud services and provide the DC-NDR-FDR replication link so as to meet the RTO and the RPO requirements mentioned in Service Level Assurance in this RFP.
- Maximum RTO shall be 2 hours and maximum RPO shall be 15 minutes for Far DR.
- In case of failover from primary site to secondary (FDR), compute environment for the critical application at FDR site shall be equivalent to DC including all the security features and components of DC, without the failover components. Development/test/quality environment will not be required at DR site.
- MSP to migrate the data from on premises to the proposed CSP.

- The MSP shall clearly define the process in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to FDR. The CSP shall plan all the activities to be carried out during the Disaster Drill and inform Ministry at least three weeks before such drill.

6. Section 6 Delivery Schedule/Timelines

S.No.	Milestone	Timelines	Payment
1	Issuance of LOI/Work Order to successful MSP	T0	Nil
2	Provisioning of required infrastructure along with Network Connectivity	T1 = T0+7 Days	Nil
3	Migration of all PESO applications to the proposed CSP Cloud Infra and Go-Live	T2 = T1 + 45 days	Nil
4	Stabilization/Operational Acceptance	T3 = T2 + 15 days	100% of migration manpower cost
5	Operation and maintenance phase	Will start from the date of stabilization/operational acceptance provided	Monthly Payment for 11 months

** Payment will be based on the actual usage of the services and as per the "Unit Cost" provided in the BOM.*

7. Payment Schedule and Commercial Bid Format

7.1 Commercial Bid Format

Sr.	Cost Head (A)	Cost (Recurring) (B)	MSP Discount in (%) (C)	Bid Price for 13 months in INR (D)
1	CSP Usage Cost per Month, including Enterprise support cost *as per BoM*	Cell No. J42 of Annexure C – CSP Public Price BoM	Applicable %	**D1= B1*(1-C)*13**
2	Manpower Charges for Migration services	Lumpsum cost	Not Applicable	**D2 = B2**
3	Per unit Hourly cost of CSP Professional Services to be taken as per requirement (on-demand basis) - 24 Hours per month	Per unit hourly cost	Not Applicable	**D3 = B3*24*13**

4	Managed Service Provider Cost for Manpower for maintenance and management of Cloud infrastructure - in percentage of Monthly CSP Usage Cost	Applicable%	Not Applicable	**D4 = D1*B4**
5	Cost of 3rd Part Security components including installation and commissioning	Lumpsum cost	Not Applicable	**D5**
6	Training and Capacity Building	Lumpsum cost	Not Applicable	**D6**
TOTAL PRICE				**P1= D1+D2+D3+D4+D5+D6**
Taxes – GST@18%				**P2 = P1*18%**
TOTAL BID PRICE				**Total Bid Price = P1 + P2**

7.2 Commercial Terms & Conditions:

1. PESO/DPIIT is free to opt for any service or configuration of service in the host of offerings of the CSP at the same rate of discount mentioned in C1 of above table.
2. For any service, which is mentioned or not mentioned in the BOQ (including any new cloud service introduced by the CSP after the tender due date), will have to be provided to PESO/DPIIT at the same discount rate as quoted in the table for the overall category.
3. PRICES VARIATION CLAUSE (PRICE ESCALATION/ DE-ESCALATION):
    f) MSP is requested to offer their best discounts over the Published/Listed Rates of the CSP as on date of the tender
    g) These Discounts shall form part of any change clause and would remain FIRM for the entire contract period.
    h) Price escalation/de-escalation shall be determined every month, based on the prevailing Published/Listed Rates in the month for which escalation is being calculated. If the Published/Listed Rates of the CSP are in USD, such rates would be converted into INR based on the published RBI reference rate of the day prior to the billing date by the MSP.
    i) Thus, the price applicable for any service in any month would be equal to Published/Listed Rates as declared by the CSP multiplied by the quoted discount rate for that particular service category.
4. SLAs / penalty, (if any) as applicable will be deducted during the monthly payment.

5. The bid value shall include all taxes and levies, except GST (Goods and Services Tax), and shall be in Indian Rupees (₹).
6. Applicable taxes would be deducted (TDS etc.) at the prevalent rates.
7. All cloud usage payments will be made on actuals as per usage report generated bill by CSP.
8. The commercial bid should include reasonable estimates of Out of Pocket (OPEs) and Other Miscellaneous Expenses which shall not be reimbursed at actuals.

7.3 Payment Schedule

Sr No	Cost Head (A)	Frequency	Payment Schedule
1	CSP cost based on Actual Usage Generated Monthly Invoice * (1- MSP Discount Quoted by MSP), including Enterprise Support)	Monthly	100% after deduction of Penalty (if any) on actuals within 15 days of submission of invoice
2	Manpower services cost for Migration	Post migration and stabilization phase	100% after deduction of Penalty (if any) on actuals within 15 days of submission of invoice
3	CSP Professional Services, as per requirement (on-demand basis)	As per billing month	100% after deduction of Penalty (if any) on actuals within 15 days of submission of invoice
4	Managed Service Charges (Cloud Management charges/ Manpower/ Maintenance.	Monthly	100% after deduction of Penalty (if any) within 15 days of submission of invoice
5	3rd Part Security components	On license procurement, delivery and installation	100% after deduction of Penalty (if any) within 15 days of submission of invoice
6	Training & Capacity Building	Once delivered	100% after deduction of Penalty (if any) within 15 days of submission of invoice

Section 8. Standard Form of Work Order

STANDARD FORM OF WORK ORDER FOR APPOINTMENT OF AGENCY

Between

[Name of client]

[Name of the AGENCY]

[Date]

I. Form of Work Order

Work order to undertake [name of assignment]

O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in

hereinafter referred to as the

-Client which expression unless repugnant to context or meaning thereof shall include its successors, affiliates and assigns) has:

a. requested the Agency to provide certain services as defined in the General Conditions attached to this work order (hereinafter called the -Services); and
b. The Agency, having represented to the Client that they have the required professional skills, personnel and technical resources, have agreed to provide the services on the terms and conditions set forth in this assignment.

NOW THEREFORE the Client hereto hereby agrees as follows:

1. The following documents attached hereto shall be deemed to form an integral part of this work order:
Appendix A: Terms of reference containing, inter-alia, the Description of the Services and reporting requirements,

Appendix B: Cost Estimate

Appendix C: Copy of Bank Guarantee for Performance Security

[in the format given in Annexure A]

Annexure A: Form of Bank Guarantee for Performance Security

(To be stamped in accordance with Stamp Act if any, of the country for issuing bank) Ref.: Bank Guarantee:

Date:

Sir,

In consideration of O/o Chief Controller of Explosives, Petroleum and Explosives Safety Organisation (PESO), A-Block, 5th Floor, C.G.O. Complex, 440 006 | Seminary Hills, Nagpur Maharashtra – 440 006 Email: explosives@explosives.gov.in (hereinafter referred as the _Client_, which expression shall, unless repugnant to the context of meaning thereof include its successors, administrators and assigns) having awarded to M/s [name of Agency] a [type of company], established under laws of [country] and having its registered office at [address] (hereinafter referred to as the _ Agency which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and permitted assigns), an Assignment for preparation of [name of assignment] Work order by issue of Client's Work order Letter of Award No. [reference] dated [date] and the same having been unequivocally accepted by the Agency, resulting in a Work order valued at Rs. [amount in figures and words] for (Scope of Work) (hereinafter called the _Work order_) and the Agency having agreed to furnish a Bank Guarantee amounting to Rs. [amount in figures and words] to the Client for performance of the said Agreement.

We [Name of Bank] incorporated under [law and country] having its Head Office at [address](hereinafter referred to as the Bank), which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators executors and assigns) do hereby guarantee and undertake to pay the Client immediately on demand an or, all monies payable by the Agency to the extent of Rs. [amount in figure and words] as aforesaid at any time up to [date] without any demur, reservation, contest, recourse or protest and/ or without any reference to the Agency. Any such demand made by the Client on the Bank shall be conclusive and binding notwithstanding any difference between the Client and the Agency or any dispute pending before any Court, Tribunal, Arbitrator or any other authority.

We agree that the Guarantee herein contained shall be irrevocable and shall continue to be enforceable until the Client discharges this guarantee.

The Client shall have the fullest liberty without affecting in any way the liability of the Bank under this Guarantee, from time to time to vary the advance or to extend the time for performance of the Work order by the Agency nor shall the responsibility of the bank be affected by any variations in the terms and conditions of the work order or other documents. The Client shall have the fullest liberty without affecting this guarantee, to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the Client and to exercise the same at

any time in any manner, and either to enforce or to forbear to enforce any covenants, contained or implied, in the Work order between the Client and the Agency any other course or remedy or security available to the client. The Bank shall not be relieved of its obligations under these presents by any exercise by the Client of its liberty with reference to the matters aforesaid or any of them or by reason of any other act or forbearance or other acts of omission or commission on the part of the Client or any other indulgence shown by the Client or by any other matter or thing whatsoever which under law would but for this provision have the effect of relieving the Bank.

The Bank also agrees that the Client at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Agency and notwithstanding any security or other guarantee that the client may have in relation to the Agencies liabilities.

This Guarantee shall be irrevocable and shall remain in full force and effect until discharge by the Bank of all its obligations hereunder.

This Guarantee shall not be affected by any change in the constitution or winding up of the Agency/the Bank or any absorption, merger or amalgamation of the Agency/the bank with any other Person.

Notwithstanding anything contained herein above our liability under this guarantee is limited to Rs. [amount in figure and words] and it shall remain in force up to and including [date] and shall extend from time to time for such period(s) (not exceeding one year), as may be desired by M/s [name of Agency] on whose behalf this guarantee has been given. Date this [date in words] day [month] of (year in _yyyy_ format] at [place].

WITNESS

1. [Signature, Name and Address]
2. [Signature, Name and Address]

[Official Address]

Designation

[With Bank Stamp]

Attorney as Per Power of Attorney No.

Dated

The date will be fixed as indicated in S.C.C. Designation

The stamp papers of appropriate value shall be purchased in the name of bank which issues the “Bank Guarantee”. The bank guarantee shall be issued by either a bank (Nationalized/Scheduled) located in India or a foreign bank through a correspondent bank (scheduled) located in India or directly by a foreign bank which has been determined in advance to be acceptable to the Client.

Annexure B: Technical Requirements – Cloud Service Provider

The compliance to the same needs to be provided on letterhead of CSP. Compliance for 3rd party security components, if any, needs to be provided on 3rd party OEM letterhead.

CSP is requested to provide compliances for requirements against the below. The template for compliance requires the following:

- Submission of Public URL highlighting Compliance to each requirement below. The template of the same is as follows:

Service Name	S. No.	Description		Compliance URL
Compute Service	1	Virtual Machines (VMs) / Compute Instances	The CSP should provide both on-demand (i.e. pay-per-hour) and long term committed virtual machines / instances for minimum of 1 year respectively	Specific URL page stating compliance requirement

General requirements

S. No.	Requirements	Compliance Y/N
1.	All CSP services listed below should be native to CSP's cloud environment.	
2.	All services provisioned by the CSP, including both DC, NDR and Far DR services, shall be provided from different data centre locations as empaneled under MeitY.	
3.	The CSP shall have the exact same configurations, including processors, managed services along with the features, compute, RAM, etc., for both DC and DR locations for the services/ infrastructure required.	
4.	CSP to deploy, configure, and manage DC and NDR sites in active-active synchronous replication mode. If not available, please declare the mode of DC/DR in asynchronous available. Please mention the data center for DC and DR. The DC and DR should offer required services at all times.	
5.	All cloud services should be launched in India region only	

Service Name: Compute Services

S. No.	Requirements		Compliance Y/N
1.	Virtual Machines (VMs) / Compute Instances	The CSP should provide both on-demand (i.e. pay-per-hour) and long term committed virtual machines / instances. Should be x86 compatible	

2.	Virtual Machines (VMs) / Compute Instances	Virtual Machine/Compute services should offer 99.99% uptime SLA with active-active architecture across data centers.	
3.	Virtual Machines (VMs) / Compute Instances	Virtual Machine/Compute services should allow to use the CPU to the fullest irrespective to the number of threads per CPU.	
4.	Self-Service Provisioning	The CSP should offer self-service provisioning of virtual machines and other services as a native service either through a programmatic interface (API/CLI) or through a management console.	
5.	Scaling automation	The CSP should support automatic launching or termination of VMs/ instances based on the parameters such as CPU utilization defined by users. The CSP should support auto scaling using custom metrics as well.	
6.		Should be available in burstable and non-burstable type	

Service Name: Relational Database Services

S. No.	Requirements		Compliance Y/N
1.	Relational Database Service	The CSP should provide/support of relational database service (MySQL, PostGre SQL) provided as native cloud service (and not marketplace) enabling handling of routine database tasks such as provisioning, patching, backup, recovery, failure detection, and repair etc.	
2.	Vertical Scaling	The CSP offered managed database service should support vertical scaling of the database instance with few clicks.	
3.	Database Storage scaling	The CSP offered managed database service should support storage auto scaling without rebooting database instance.	
4.	Database horizontal scaling	The CSP offered managed database service should support up to 10 read replicas to horizontally scale reader nodes.	
5.	Database horizontal auto-scaling	The CSP offered managed database service should be able to dynamically adjust the number of Read Replicas to handle sudden increases in connectivity or workload.	
6.	Database Storage IOPS scaling	The CSP should support provisioning of additional IOPS for database storage without forcing to increase the disk size of the provisioned storage.	
7.	Database backup	The CSP offered managed database service should ensure that no performance impact or interruption of database service occurs as backup data is being written.	

8.	Serverless compute invocation	The managed database service of the CSP should be able to invoke serverless compute from database code	
9.	Database high availability	The managed database service of the CSP should provide High Availability mode i.e. should support automatic failover to other database node without manual intervention.	
10.	Database Blue-Green deployment	The managed database service of the CSP should provide support for Blue-Green deployment for database changes as native capability.	
11.	Point-In-Time recovery	The managed database service of the CSP should support Point-In-Time recovery to restore the database cluster to a specific point in time	
12.	Database Cloning	The managed database service of the CSP should support database cloning to fast create a new DB cluster from original cluster.	

Service Name: Storage Services

Block Storage			
S. No.	**Requirements**		**Compliance Y/N**
1.	Support for storage allocated as local disk to a single VM	The CSP should offer block level storage volumes for use with VMs / compute instances.	
2.	Storage Volumes	The CSP should offer block storage volumes greater than 1 TB in size. CSP should allow to increase the capacity of single managed disk in 1GB incremental size for both application and database block storage. The CSP should charge only for the provisioned block storage capacity.	
3.	Auto scaling of block storage	CSP should allow auto scale of storage capacity based on usage without reboot of VM for any size of block storage volume.	
4.		The CSP offered block storage disks should allow to increase the size without either deallocating the VM or detaching the disk.	
5.		The Selected Bidder shall provide SSD based block storage capabilities on- demand, dynamically scalable per request, for VM & Server instances, of arbitrary size ranging from 1 GB to multiple TBs. Once mounted, the block storage should appear to the virtual machine like any other disk.	
6.	Block Storage configuration	The CSP should support creating the block storage volume of any size rather than pre-defined configuration.	
7.	I/O support	The CSP should offer minimum - 3 IOPS per GB of block storage for applications - 6,000 IOPS per volume for DB Storage volume size	

		upto 1TB. - Min 10,000 IOPS per volume for volume size above 1TB.	
8.		The CSP offered SSD block storage should support OS disk usage.	
9.		The CSP offered SSD block storage should support backup from CSP's native backup service.	
Object Storage			
1.	Scalable object storage service	The CSP should offer secure, durable, highly-scalable object storage for storing and retrieving large amount of data. The data should automatically be stored in at least 2 different data centers to ensure high durability.	
2.	Object lifecycle Management	The CSP should offer native capability to manage an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to archival to deletion	
3.	Parallel / Multi part upload	The CSP should support uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.	
4.	Data Security	Data at rest in various Data stores should be protected by hashing confidential data in both transactional and warehouse data stores. The security for the transactional data stores must be ensured.	
5.	Automatic storage tiering	The CSP should offer object storage with the capability to monitor access patterns and automatically move objects that have either been accessed infrequently or never accessed to lower-cost access tiers.	
Archival Storage			
6.	Archival Storage	The CSP should offer low cost archival storage to store long-lived data.	
7.	Archival Storage retrieval	The CSP should offer ability to retrieve archived data.	
8.	Archival Storage minimum duration	The CSP offered archival storage should support minimum object duration of 180 days or less.	
File Systems			
9.	SSD based file system	The CSP should offer fully managed SSD backed file system.	
10.	Data durabilit	The Storage in the CSP offered File System to automatically be backed across data centers that are in different physical	

	y and redundancy.	location (distinct and independent infrastructure) to avoid common points of failure across Data centre (Zone Redundant).	
11.	File System supported protocols	The CSP offered File System should be accessible by using NFS, SMB, and iSCSI protocols.	
12.		The CSP offered managed File System should provide consistent sub-millisecond latencies.	

Service Name: Security Services

S. No.	Requirements		Compliance Y/N
1	Identity and Access Management	The CSP should have native capabilities to securely control access to services and resources for the users.	
		CSP should have native abilities to create and manage users.	
		CSP should have native capabilities to create roles and groups.	
2	Threat Detection	The CSP should offer a native fully managed threat detection service.	
		Native capabilities to continuously monitor for malicious or unauthorized behavior.	
		Native capabilities to analyze billions of events across multiple accounts using machine learning to detect anomalies.	
		The native threat detection service should be able to generate actionable alerts.	
		The native threat detection service should support integration with existing event management and workflow systems.	
3	Security Assessment Services	The CSP should offer a native service for automated security assessment.	
		Native service to help improve the security and compliance of applications deployed on the cloud.	
		Native service to automatically assess applications for exposure, vulnerabilities and deviations from best practices.	
		Service should be able to produce a detailed list of security findings prioritized by level of severity.	
		Should be able to check for unintended network accessibility and vulnerabilities of the VMs.	
		Should offer pre-defined rules packages mapped to common security best practices and vulnerability definitions.	
		Rules should be regularly update by the CSP.	

S. No.	Requirements		Compliance Y/N
5	Data Protection Service	The CSP should have a native, fully managed data security and data privacy service.	
		The native data security service should be able to automatically discover, classify, and protect sensitive data in cloud.	
		Native support to recognizes sensitive data such as personally identifiable information (PII) or intellectual property using machine learning.	
		Should provide dashboards and alerts to give visibility into how this data is being accessed or moved.	
		Should be able to continuously monitor data access activity for anomalies detection.	
		Should be able to generates detailed alerts when risk of unauthorized access or inadvertent data leaks are detected	
8	Firewall Management	The CSP should offer a native security service to centrally configure and manage firewall rules.	
		The native security service should be able to configure firewall rules across multiple accounts and applications.	
		The native security service should provide a mechanism to easily roll out firewall rules.	
		The native security service should be able to support new applications and resources into compliance with a common set of security rules from day one.	
		The native security service should provide a single place to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner.	
9	Encryption Key Management	The CSP should offer a native, fully managed service to create and manage encryption keys.	
		The native, fully managed key management service should be able to control encryption across a wide range of cloud services and applications.	
		The native, fully managed key management service should be FIPS 140-2 Level 3 complaint.	
		The native fully managed key management service should be able to provide the logs of all key usage to help meet our regulatory and compliance.	
11	DDoS Protection	The CSP should have a native managed service to protect against Distributed Denial of Service (DDoS) attacks.	
		The DDoS solution should be able to protect 500 resources	
		The native managed DDoS protection service should provide always-on detection and automatic inline mitigations that minimize application downtime and latency.	

S. No.	Requirements		Compliance Y/N
13	Web Application Firewall	The CSP should have a highly available native web application firewall.	
		The native web application firewall should be able to protect the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.	
		The native web application firewall should be able to give us control over which traffic to allow or block the web application by defining customizable web security rules.	
		The native web application firewall should support creation of new custom rules that block common attack patterns, such as SQL injection or cross-site scripting and rules that are designed for our specific application.	
		Should autoscale to support load as per requirement and with redundant feature	
		The native web application firewall should be able to deploy new rules immediately.	
14	KMS for DB Encryption	The solution must support full key lifecycle operations, including secure key generation, storage, rotation, archival, and destruction (CRUD operations).	
		The solution should have the capability for providing the Transparent encryption software agent for Block Cipher encryption. Should support operating systems like, SUSE Linux, RHEL, CentOS, Windows. The encryption software module should have independent FIPS 140-3 level 1 certification.	
		The solution should be capable of providing External Key management in case native encryption for the databases (MS SQL, Oracle) is being used	
		The solution must support REST APIs for encryption, decryption, digital signing, and key access.	
		The solution must support High Availability (HA) and should be deployable in Active- Active in both DC and DR Environments	
		The solution must integrate with enterprise identity providers such as LDAP, Active Directory (AD), Single Sign-On (SSO), and Multi-Factor Authentication (MFA).	
		The solution must provide a centralized administrative console with Role-Based Access Control (RBAC). The solution must support fine-grained access policies for key usage, including user, application, and operation-level controls.	

S. No.	Requirements		Compliance Y/N
15	DAM (Database Activity Monitoring)	Each Gateway/Collector of the DAM solution shall consistently support a high throughput of at least 60,000 Transactions Per Second (TPS) for all database queries, including those involving sensitive objects and privileged users, without any performance degradation or differentiation based on the nature or privilege level of the SQL activity.	
		The proposed solution should support both agent and agentless based mode depending on the database type, its placement etc…	
		The Solution should have Risk Analytics and must be available in the following offerings with pre-hardened Unix OS - Virtual appliance (VMware or Hyper-V) - Amazon Web Services (AWS) EC2 Supported	
		The Risk Analytics Solution should provide an intuitive dashboard page containing widgets that give a quick informative and drill down capabilities view of the following: a) Protected Assets b) Open Issues c) Security Events Over Time d) Entities With Most Severe Incidents e) Events Analyzed f) System Health Status	
		The Risk Analytics Solution must be able to support the identification of anomalous activity based on DAM monitoring for databases including, - DB2 LUW - MSSQL - Oracle - Sybase ASE - Teradata	
		The solution should support the following authentication mechanism for accessing the solution:	

S. No.	Requirements		Compliance Y/N
		(i) In-built authentication in the solution (ii) Kerberos authentication (iii) LDAP/AD authentication (iv) RADIUS authentication	
		The Proposed Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.	
		The proposed solution should support more than 200 database types including the categories of 1. Conventional Databases 2.In-Memory databases 3.Application in-build databases 4. Big Database types 5. Data lakes 6. Cloud based databases	
		Solution should provide risk score of individual databases, based on combination of security alerts, discovery results, vulnerability assessment, sensitivity & confidentiality of data stored in the database.	
		Solution should provide good compression ratio upto 10:1 to store logs which will require minimum infra and should have ability store the log online for multi year retention requirement	

Managed API Gateway

S.No.	Requiremnts		Compliance Y/N
1	Availability and Scalability	The proposed Managed API Gateway should be CSP managed and should be highly available (minimum 99.95% availability) and scalable	
2	Supported APIs	The proposed Managed API Gateway should support REST, HTTP and WebSocket APIs.	
3	Caching	The proposed Managed API Gateway should support 5 GB of caching	
4		API Gateway should support a minimum of 5,000 transactions per second to manage peak load	

5		The CSP should offer a managed service for API security such as HTTPS/ SFTP hosting and allow configuration of API throttling	
6		API Gateway should support API throttling.	

Service Name: Network Services

S.No.	Requiremnts		Compliance Y/N
1	NAT Gateway	1. Managed NAT Gateway. 2. Should be Highly Available.	
2	Subnet level filtering (Network ACLs/ Security Groups)	The CSP should support subnet level filtering – Network ACLs /Security Groups that act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.	
3	Ingress filtering	The CSP should support adding or removing rules applicable to inbound traffic (ingress) to instances.	
4	Egress filtering	The CSP should support adding or removing rules applicable to outbound traffic (egress) originating from instances.	
5	Site-to-Site IPSec VPN service	The CSP should support Site-to-Site IPSec VPN connection between the cloud provider and customer data centre.	
6	Application Load Balancing of VM	Application load balancer for Layer 4 and Layer 7 and Should be highly available	
7	Domain Name Registration (DNS)Service	The CSP should provide a scalable and highly available DNS service.	
8	Content Delivery Network (CDN)	CSP Managed CDN with - Support for HTTP/2, HTTP/3, TLS 1.3 with security features including DDoS protection, CSP's WAF managed rulesets and SSL certificate management. - Native integration with CSP Object Storage and Services -Supprt for Edge computing with custom code execution at PoPs. - Support to securely deliver audio, video, images, data, application, etc from single distribution - CSP should have PoP available in Tier1/2/3 city - Private Link support for connecting to Origins like Load balancers	

Service Name: Visualization/ Analytics/ AI/ML Services

Service	Description	Compliance Y/N
Managed Data Warehouse	Compatible with structured and semi structured data	
	Should support concurrency scaling. Concurrency scaling for daily 1 hr shall be free of cost	
	Automatic and Manual table optimization should be supported	
	Ability to run SQL queries against semi-structured/unstructured data	
	Should provide ML Model Training using SQL as an in-built service with free inferences	
	Should Support native integration with Spark	
	Should support Zero ETL With Postgres and MySql	
	Should be placed inside a VPC	
	Should be available in both serverless and Cluster mode	
Managed Data Lake Capability	Should be able to Scale to 100+ nodes	
	Data Lake should support ACID Operations natively	
	Should support rowlevel and Column level security	
	Should support Data mesh Architecture	
	Should support open format like Json, Parquet, ORC.	
	Should support various compression technique(E.g- Snappy,Gz)	
Interactive Query Service	Supports querying almost all open-source file formats like, Parquet, Avro, ORC, Delta lake, JSON and Delimited file	
	Query history & result caching – faster response at no extra cost	
Managed ETL	Supports Spark, Python Shell, & Ray	
	Should support Streaming ETL	
Managed Visualisation tool	CSP should offer a native serverless BI visualization service with on per user and per view basis.	
	BI visualization service should provide both in-memory data storage and connection to different data sources for dashboard queries natively.	
	BI visualization service should provide drag and drop feature, data filtering and feature engineering capabilities to create visualization.	

Service	Description	Compliance Y/N
	BI visualization service should provide machine learning based automatic trend identification in data	
	BI visualization service should provide linking of charts, multiple pages/tabs in a dashboard to group different types of charts in a dashboard	
	BI visualization service should support asking questions in natural language and receive answers with relevant visualizations	
	BI visualization service should automatically scale based on number of users and dashboard access.	
	BI visualization server should allow both row level and column level security	
	Should support embedding of Reports without Iframe natively	
	Should be able to Embed Report Authoring UI natively	
Managed Machine Learning Platform as a Service	Managed Jupyter Notebook for Machine Learning	
	Fully Managed Machine Learning Instance for Training Models (with GPU Linux)	
	Fully Managed Machine Learning Instance for Inference (with GPU Linux)	
	Fully Managed Machine Learning Instance for Inference (with GPU Linux)	
	Centralized managed Feature Store to manage machine learning features	
	Managed machine learning solution to build workflow for human review of ML output	
Generative and Agentic AI	Frontier LLMs available for in-country inferencing	
	Unified Converse API across multiple models	
	Framework-agnostic runtime for agent runtime	
	Fully Managed Machine Learning Instance for Inference (with GPU Linux)	
	Model-agnostic guardrails via standalone Apply Guardrail API	
	Availability of Zero Operator Access (ZOA) model	

3rd party Security components, if any, required to be provisioned for meeting above mentioned technical compliances cannot be offered through CSP Marketplace. The bidder must submit the Authorization from the OEM of 3rd party Security components. In case of non-submission of authorization, the bid will be summarily rejected.

Annexure C: Publicly Listed Prices of CSP (To be submitted along with technical bid)

S. No	Item/Specification	Type/Configuration	Type	Unit of measurement	Cost Calculator Link to highlight derived unit CSP listed cost (should be as certified by CSP - refer technical requirement)	Quantity	Indicative Hours	Public Unit Price of proposed CSP (USD)	Total Public Price of the proposed CSP (USD)
1	Virtual Machine	16 vCPU 64 GB RAM, x86-64 Processor, Linux OS, Non-burstable	On-Demand	per Hour		10	200		0
	Virtual Machine	16 vCPU 64 GB RAM, x86-64 Processor, Linux OS, Non-burstable	1 Year Reserved Pricing with no upfro	per Hour		30	730		0

			nt pay ment						
	Virtual Machine	8 vCPU 32 GB RAM, x86-64 Processor, Windows OS, Non-burstable	On-Dem and	per Hour		5	200		0
	Virtual Machine	8 vCPU 32 GB RAM, x86-64 Processor, Windows OS, Non-burstable	1 Year Rese rved Prici ng with no upfro nt pay ment	per Hour		10	730		0
2	Disk Storage	Single Solid State Drive (SSD) Volume of 500 GB without Disk Striping with 3000 IOPS & 125 MB/Sec throughput offering single-digit millisecond latency. - Disk can be used as both OS Disk and Data Disk	On-Dem and	per month		200	NA		0
3	File Storage	Fully managed shared storage file system, enabling multi-protocol access standard NFS, SMB, iSCSI, and NVMe-over-TCP protocols and automated storage tiering	On-Dem and	per TB per Month		50	NA		0
	Object Storage	Managed Hot Object Storage at DC with data redundancy across 3 physically distant MeitY empanelled sites	On-Dem and	per TB per Month		20	NA		0

4	Retrival SLA	Retrival SLA should be within 48hrs	On-Demand	Per TB Per month		50	NA		0
	Archival Storage	Managed Archival Storage with data redundancy across 3 physically distant MeitY empanelled sites. Minimum duration should not be more than 180 days	On-Demand	per TB per Month		300	NA		0
5	Managed Relational Database	Managed MS SQL as a service: (Non burstable) 16 vCPU 64 GB RAM, MS SQL Ent. edition -HA and horizontal read scaling by adding/ removing multiple read replicas across physically distant MeitY empanelled sites - storage auto scaling based on the workload demand -Support for Point In Time log retention for 30 days	On-Demand	per Hour		1	200		0
	Managed Relational Database	Managed MS SQL as a service: (Non burstable) 16 vCPU 64 GB RAM, MS SQL Ent. edition -HA and horizontal read scaling by adding/ removing multiple read replicas across physically distant MeitY empanelled sites - storage auto scaling based on the workload demand -Support for Point In Time log retention for 30 days	1 Year Reserved Pricing with no upfront payment	per Hour		1	730		0

	Managed Relational Database	Fully Managed PostgreSQL Database Engine: (Non burstable) 32 vCPU 256 GB RAM -HA and horizontal read scaling by adding/ removing multiple read replicas across physically distant MeitY empanelled sites - storage auto scaling based on the workload demand -Support for Point In Time log retention for 30 days - Support for native Blue green upgrades	On-Demand	per Hour		2	200		0
	Managed Relational Database	Fully Managed PostgreSQL Database Engine: (Non burstable) 32 vCPU 256 GB RAM -HA and horizontal read scaling by adding/ removing multiple read replicas across physically distant MeitY empanelled sites - storage auto scaling based on the workload demand -Support for Point In Time log retention for 30 days - Support for native Blue green upgrades	1 Year Reserved Pricing with no upfront payment	per Hour		6	730		0
6	Application Load balancer	CSP native layer 7 Load balancer supporting SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancer evaluating 50 rules for	On-Demand	Per Month		8	NA		0

		every request with data processed upto 1 TB/month. Should support zone redundancy, autoscaling & association with WAF							
7	API Gateway	CSP Managed API Gateway processing 10 million REST API calls per month - Should provide a fully managed production grade serverless service for publishing APIs to external and internal consumers. - Must not need any provisioning of underlying compute, external proxy, or external cache. - Should support REST requests with rate limiting and in-built caching. - Should come with Autoscaling & Availability zone support (deployment across physically distant MeitY empanelled sites) - Should support security features (protection from malicious clients & abuse) & analytics reporting (response time, latency, error rate, cache hit count etc.) - Should be able to handle upto 10,000 requests per seconds	On-Demand	per API Gateway per month		8	NA		0

8	MQ	CSP Managed Rabbit MQ cluster with 3 brokers deployed across physically distant MeitY empanelled sites - Data Encryption of messages at rest with customer managed keys and transit with support for TLS 1.2 & 1.3 -Private networking with VPC/Vnet -Configuration of each broker: 4 vCPU/ 16 GB RAM)	On-Demand	per cluster per hour		2	730		0
9	OpenSearch Service	CSP Managed OpenSearch cluster deployed across physically distant MeitY empanelledsites - Support for master and data node separation, warm/cold storage tiers,cross cluster replication and vector database capabilities for Gen AIworkloads. - Support private VPC/VNet connectivity, encryption at rest usingCustomer Managed Keys and encryption in transit. Configuration: 4vCPU/ 32GB RAM	On-Demand	per node per hour		2	730		0
10	Caching Layer	Redis/Valkey engine v7 and above. Should support clustering, replication and automatic failover across physically distant MeitY empanelled sites. - Should have Inbuilt capability to auto scale	On-Demand	per node per hour		7	730		0

		number of shards and read replicas based on scaling policy Configuration: 4 vCPU/ 16 GB RAM							
11	Networking	Fully managed Point to Site VPN providing secure access to remote users supporting encrypted TLS connections, multi-platform clients (Windows, macOS, Linux)	On-Demand	per VPN connection per hour		1	730		0
			On-Demand	per active client connections per hour		10	730		0
	Networking	Fully managed Site to Site VPN: VPN Connectivity as Site-to-Site VPN with two tunnels across multiple Availability zones. Support upto 1.25 Gbps of bandwidth	On-Demand	Per VPN per Hour		26	730		0
12	Centralized Firewall Management	Centralized security management service to configure and maintain security policies (Network Firewall, WAF, Security Groups) across multiple accounts. - Support automated policy enforcement i.e. deployment of baseline WAF, Network Firewall rules, remediation and comprehensive compliance reporting.	On-Demand	per policy per month		2	NA		0

13	Web Application Firewall	CSP managed Web Application Firewall with HA across physically distant MeitY empanelled sites - 10 rules processing 100MN hits & 10 TB data processing per month - Should provide CSP managed rules for Threat Intelligence for blocking requests based on IP repuation list (Tor nodes, Public Cloud IPs, VPNs, known malicious IPs) , bot protection with real time metrics - Support native Integration with Application Load Balancer, API Gateway and CDN	On-Demand	per WAF per month		5	NA		0
14	Managed Network Firewall	CSP managed Network Firewall with IPS capabilities • Should support TLS inspection Configuration: 1 Firewall endpoint with 1 TB data inspection per month	On-Demand	per Firewall endpoint per month		3	NA		0

15	Content Delivery Network	CSP Managed CDN with - Support for HTTP/2, HTTP/3, TLS 1.3 with security features including DDoS protection, CSP's WAF managed rulesets and SSL certificate management. - Native integration with CSP Object Storage and Services -Supprt for Edge computing with custom code execution at PoPs. - Support to securely deliver audio, video, images, data, application, etc from single distribution - Private Link support for connecting to Origins like Load balancers without additional proxy/VPN - Pay-as-you-go model to be quoted only	On-Demand	per TB per month		20	NA		0
16	Public IP	CSP provided static Public IP reachable over Internet	On-Demand	per IP per month		10	NA		0
17	Data Transfer	Data Transfer Out to Internet	On-Demand	per TB per month		2	NA		0
18	NAT Gateway	Network Address Translation (NAT) Gateway with 30 GB processing per month -Should support connecting to 50 Virtual machines	On-Demand	per month per NAT		3	730		0
19	Container Registry	CSP Managed container registry with OCI, Should support vulnerability scanning on image push,	On-Demand	per month per TB		2	NA		0

		customer managed keys, and cross-region replication							
20	Code Pipeline	Managed continuous delivery pipeline service for automating application release workflows.	On-Demand	pipeline per account / month		3	NA		0
21	Anti DDoS	Managed DDoS Service provides L3, L4 and L7 application protection, expert guidance from response team during active DDoS incidents, cost protection to safeguard against scaling charges resulting from DDoS-related usage spikes Total resources to be protected:300	On-Demand	per month		1	NA		0
22	Streaming Service	Managed Cloud native Streaming for Apache Kafka (MSK), 2 vCPU, 8 GB RAM with 100 GB Storage For serverless offering: Up to 20 MB/s aggregate ingress, 40 MB/s egress, supporting up to 1,000 partitions	On-Demand	per node per hour		2	730		0

23	Data Warehouse	- CSP Managed enterprise data warehouse (EDW) to run complex queries across petabytes of data. - Support creation, auto refresh & querying of materialzed views, automatic workload management with concurrency scaling - Support HA cluster deployment & auto failover across physically distant MeitY empanelled sites - Support Data Governance features including Row level Security , Data Masking, and cluster encryption using Customer Managed Key Data Warehouse: 4vCPU, 32 GB RAM, 10 TB storage or equivalent serverless offering supporting 300 queries per month each processing 1 TB of data	On-Demand	per node per hour		3	730		0
24	Vulnerability Scanning	AI/ML-powered continuous security monitoring service providing threat detection across cloud accounts, containers, and storage services without additional infrastructure deployment. - Support severity-based findings	On-Demand	per node per month (each node with 2 vCPUs)		200	NA		0

		(Critical to Low), MITRE ATT&CK® framework correlation, and automated detection of reconnaissance activities, account compromises, and malware scanning of block storage & obect storage. - Runtime Monitoring of Compute, Container workloads - Support for Organization wide threat aggregation and integration with CSP's CSPM.	On-Demand	per GB of Data volume for malware scanning		1000	NA		0
25	Encryption Keys	Fully managed Key Management Service backed by CSP's HSM to create and control the keys used for cryptographic operations Compliance with FIPS 140-3 Level 3.	On-Demand	per key with 10000 symmetric requests per month		20	NA		0

26	Managed AI Inference Platform	1. Platform shall provide a unified managed AI environment for developing, fine-tuning, deploying, monitoring, and governing AI/ML models, GenAI applications, and AI agents. 2.Service shall support access to foundation models, open-source LLMs, embeddings, and AI agent frameworks through a centralized model catalog. 3. Platform shall support end-to-end MLOps/LLMOps including experimentation, model versioning, CI/CD pipelines, automated deployment, monitoring, evaluation, and lifecycle management. 4. Service shall provide enterprise-grade security, governance, Responsible AI controls, RBAC, audit logging, compliance management, and deployment governance across environments. 5. Platform shall support integration with AI services, vector search, RAG pipelines and enterprise data sources, APIs for	On-Demand	per node per hour		4	730		0

		production-scale AI workloads. Configuration:AI Inference Nodes, 8vCPU, 32 GB RAM with NVIDIA L4 or newer generation GPU with 24 GB of memory.							
27	GPU Instance for Training & Inferencing	CSP managed platform offering GPU with self-hosted and open source models from multiple publishers - In-built training plan feature for the models - Support deployment of models as end-points - Managed orchestration of large scale AI training, Inference - Non-burstable, production-grade compute, with enterprise class NVIDIA GPU acceleration (equivalent to L4 or latest)	On-Demand	per node per hour		16	730		0

		- Configuration: 16 vCPU, 64 GB RAM with 24 GB of GPU memory							
28	Enterprise Support	Monthly	On-Demand	On total bill of material			730		
								TOTAL	0

IMPORTANT NOTES:
1. No cells in above table that are colored should be tampered with.
2. Ministry at its sole discretion may alter (increase/decrease) quantity or may remove item . The above BoM represents no commitment towards usage as per BoM and Ministry has the right to leverage services as per requirement
3. Any wrongly mapped service/configuration of CSP for price bidding purpose not offering functionalities as mentioned in Annexure will result in disqualification at the commerical bid stage. Ministry shall compare offered service name and machine for said functionalities through calculator link above shared for each data center
4. One Month is equivalent to 730 hours for purpose of calculations in above BoM
5. Bidders should submit calculator for publicly listed prices that should match with listed price column of cost sheet. This is mandatory to compare unit cost for each service against required BoM. In case of non-availability of specific configuration, the closest highest configuration shall be submitted by bidder. Any lower configuration quoted by bidder shall lead to disqualification. Comments section may be usedd to provide any additional details related to service proposed that helps establish compliance to required BoM and functionality
6. Exchange Rate to be used in case of USD costing as 1USD=95 INR
7. In case a service is not listed on calculator of CSP, publicly listed prices of the CSP for the service needs to be provided - hyperlink of the same may be included in column F of above template. Ministry has the right to validate the services availability from the Console of CSP.
8. All above services should be that of CSP except any third party mentioned
9. Compute, Managed Databases and Storage services should be native to the proposed CSP environment
10. All compute OS and managed DB licenses (if applicable) shall be provided as part of hourly cost of CSP as per format. License cost shall not be considered as upfront cost in any manner by bidders

11. On Demand cost should be based on per hour cost with zero usage commitment in the month. The calculator submitted should be for per hour cost only while such unit rate shall be multiplied as per guidance in relevant section
12. All proposed machines shall be present in the proposed DC/DR region

Annexure- D

Bill of Material for 3rd party Security Components								
S. No	**Item/Specification**	**Type/Configuration**	**Type**	**Unit of measurement**	**Quantity**	**Unit Price (INR)**	**Total Price (INR)**	**Remarks**
1	Database Activity Monitoring Software	No. of Databse instances	License	per DB instance	10		-	
2	KMS for DB TDE Encryption	Dedicated virtual appliance	License	per virtual appliance	4		-	
4	One time Installation and Commissioning cost				1		-	
TOTAL							-	