(A Government of India Enterprise)

You focus on exports. We cover the risks.

REQUEST FOR PROPOSAL

FOR

APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED

Ref: ECGC/Tender-03/IT/09/2024-25

Date: 06.09.2024

Index

Table of Contents

Section 1

1. Introduction

1.1 Invitation to Bidders

ECGC Ltd. (Formerly Export Credit Guarantee Corporation of India Ltd.), wholly owned by Government of India, was set up in 1957 with the objective of promoting exports from the country by providing Credit Risk Insurance and related services for exports.

With this Request for Proposal ('RFP') Document (hereinafter also referred to as 'the Bid Document' or 'the Tender Document') ECGC Limited (hereinafter referred to as 'ECGC / the Company'), invites competitive Bids from vendors (hereinafter referred to as ('the Bidder(s)'.) for **"APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED"**

The "Eligibility, Technical, and Price/Financial Bids" along with the supporting documents would be received in physical form.

The Bidder(s) are advised to study the Tender Document carefully. Submission of Bids shall be deemed to have been done after careful study and examination of the Tender Document with full understanding of its implications.

The Bid Document may be downloaded from the Company's website https://main.ecgc.in/english/tenders-called-for/. Please note that all the required information asked needs to be provided. Incomplete information may lead to rejection of the Bid. The Company reserves the right to change the dates mentioned in this RFP Document, which will be communicated to the Bidder(s), and shall be displayed on the Company's website. The information provided by the Bidder(s) in response to this RFP Document will become the property of ECGC and will not be returned. ECGC reserves the right to amend, rescind or reissue this RFP Document and all SUBSEQUENT amendments, if any. Amendments or changes shall be displayed at ECGC's website only.

1.2 Schedule of events

Tender Number	**ECGC/Tender-03/IT/08/2024-25**
Mode of Tender	**ECGC Portal/ CPPP Portal** https://main.ecgc.in/english/tenders-called-for/
Date of Notice Inviting Tender (NIT) available to parties to download/ Issue of RFP Document	06th September 2024
Bid Document Availability	The Bid Document can be downloaded from website/ CPPP portal up to 26th August 2024
Last date and time for receipt of mail queries for clarification from bidders	20th September 2024 till 15:00 hrs
Earnest Money Deposit (EMD)	₹ 5,00,000/-
Date and Time of Pre-Bid Meeting & Walkthrough of existing DC setup for bidders	25th September 2024 11:00 hrs Venue: ECGC Bhawan, CTS No. 393, 393/1-45, M.V. Road, Andheri (East), Mumbai, PIN 400069, Maharashtra, India.
Date & Time of Final Submission of Eligibility, Technical, & Financial Bids along with EMD	30th September 2024 till 15:00 hrs
Date and Time of Eligibility Bid Opening	3rd October 2024 15:00 hrs
Date and Time of Technical Bid Opening	14th October 2024 15:00 hrs
Technical Bid Presentation Before the Committee	Date and time shall be intimated later
Completion of Technical evaluation	Date and time shall be intimated later
Opening of Price/ Financial Bids	Within fifteen days after opening of Technical Bids

Closure of RFP process	Post award of contract and on-boarding of selected bidder.
Contact Details: Deputy General Manager (Information Technology): 022-66590650 Deputy Chief Technology Officer (Information Technology): 022-66590764 Manager (Information Technology): 022-66590654	
Address for Communication and submission of Bid.	ECGC Bhawan, CTS No. 393, 393/1-45, M.V. Road, Andheri (East), Mumbai, PIN 400069, Maharashtra, India.
Telephone	022-66590654,651,653
All correspondence / queries relating to this RFP Document should be sent to / through following email ID only	it-tender@ecgc.in

NOTE: Timelines are subject to change at the sole discretion of ECGC Ltd.

Section - 2

Disclaimer

The information contained in this RFP Document or information provided subsequently to Bidder(s) in documentary form by or on behalf of ECGC, is provided to the Bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP Document is neither an agreement nor an offer and is only an invitation by the Company to the interested parties for submission of Bids. The purpose of this RFP Document is to provide the Bidder(s) with information to assist the formulation of their bids.

This RFP Document does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP Document and where necessary obtain independent advice.

The Company may in its absolute discretion, but without being under any obligation to do so, update, amend, supplement the information or withdraw this RFP Document at any stage. No contractual obligation whatsoever shall arise from the RFP process until a formal contract is signed and executed by duly authorized representatives of the Company with the selected Bidder.

Section - 3

Instructions for Bidder(s)

3.1 General Instructions

3.1.1 Before bidding, the Bidder(s) are requested to visit the ECGC website https://main.ecgc.in/english/tenders-called-for/ and also carefully examine the Tender Document and the General Terms and Conditions of the Contract (TCC) contained therein, and if there appears to be any ambiguity or discrepancy between any terms of the Tender Document and the Contract, they should immediately refer the matter to ECGC for clarifications.

3.1.2 The Bidder, for the purpose of making the Bid, shall complete in all respects, the form(s) annexed to the Tender Document, quote the prices and furnish the information/ documents, called for therein, and shall sign and date on each of the forms/documents in the space provided therein for the purpose. The Bidder shall affix its initial on each page of the Bidding Documents.

3.1.3 The Bid shall be signed by a person or persons duly authorized by the Bidder with signature duly attested. In the case of a body corporate, the Bid shall be signed by the officers duly authorized by the body corporate with its common seal duly affixed. In case of a consortium, the Bid shall be signed by the officer(s) so authorized by each consortium member and the Bid shall be affixed with the common seals of each member of the consortium.

3.1.4 The Bid shall contain the address, Tel. No., Fax No. and e-mail id, if any of the Bidder, for the purposes of serving notices required to be given to the Bidder in connection with the Bid.

3.1.5 The Bid form and the documents attached to it shall not be detached from one another and no alteration or mutilation (other than filling in all the blank spaces) shall be made in any of the forms or documents attached thereto. Any alterations or changes to the entries in the attached documents shall only be made by a separate covering letter otherwise it shall not be entertained for the Bidding process.

3.1.6 The Bidder, irrespective of its participation in the bidding process, or its outcome shall treat the details of the documents as privileged, secret and confidential.

3.1.7 ECGC does not bind itself to accept the lowest of any Bid and has the right to reject any Bid without assigning any reason whatsoever. ECGC also reserves the right to re-issue the Tender Document, or cancel the entire Tender process without assigning any reason(s).

3.1.8 Bids shall be submitted in three parts i.e. (1) Qualification/ Eligibility Bid (2) Technical Bid and (3) Price/Financial Bid.

3.1.9 The Bidder shall submit the **Eligibility Bid** as per the form provided under Annexure – 1 and the same shall be enclosed in a separate single sealed envelope with all supporting documents whatever.

3.1.10 The Bidder shall submit the **Technical Bid** as per the forms provided under Annexure - 4 **(A to B)** and the same shall be submitted in a separate single sealed envelope.

3.1.11 The Bidder shall submit the Price/Financial Bid as per the form provided under Annexure – 5 and the same shall be enclosed in a separate single sealed envelope.

3.1.12 Supporting documents are to be submitted in the Eligibility, Technical as well as Price/Financial Bids. Incomplete or partial submission of relevant documents will lead to disqualification.

3.1.13 The rates should be sent only in the prescribed format. Non-conformance or quotations received in any other format may result in rejection of the Bid.

3.1.14 The Bidder should ensure that there are no cuttings, over-writings, and illegible or undecipherable figures to indicate their Bid. All such Bids may be disqualified on this ground alone. The decision of the Company shall be final and binding on the Bidder. The Bidder should ensure that ambiguous or unquantifiable costs / amounts are not included in the Bid, which would disqualify the Bid.

3.1.15 Each Bidder can submit only one Bid.

3.1.16 No queries or change in requirements specifications/line items will be entertained in terms of the Bid process, except if such changes are advised or are approved by the Company.

3.1.17 The Bidder should commit to provide the resources desired by the Company for the entire duration of the engagement, at the agreed cost and terms and conditions.

3.2 Cost of Bidding

The Bidder shall bear all costs associated with the preparation and submission of its Bid, and the Company will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Bidding process.

3.3 Scope of Work for System Integrator (SI)

ECGC is looking for establishing its Disaster Recovery Centre at NTT Bengaluru. ECGC wishes to appoint a System Integrator company for Supply, procurement, implementing and managing the Infrastructure for its IT application system on turn-key basis for five years period. The scope of work broadly includes following,

3.3.1 The SI requires setting up of a full-fledged Disaster Recovery Data Center (DRDC) at NTT Bangalore.

3.3.2 The SI should prepare and submit a detailed implementation plan as per the project scope.

3.3.3 SI will be required to implement DR at NTT Bengaluru Disaster Recovery center site as per the specifications given for the data center components in the tender document. (Annexure –4) A and B

3.3.4 SI needs to setup the DRDC incorporating the appropriate requirements for Space, Rack, cooling, Power, etc. requirements for the BOM requested for setting up DR Site for ECGC.

3.3.5 The hardware requirements (BOM) for DR environment as per internal sizing done, is given as a part of tender document (Annexure – 4. A to B).

3.3.6 The SI will be required to propose optimized solution for implementation of the same including any additional infrastructure required for DR Data Centre environment setup indicating as mandatory or optional items clarifying the technical and operational usefulness of the same.

3.3.7 ECGC desires to implement Warm DR site for its business-critical / all applications with Active – Passive configuration between DC (NTT Mumbai) and DR. The data to be replicated at DR site.

3.3.8 SI needs to propose the replication techniques between DC and DR including the frequency of replication. SI shall estimate the bandwidth requirement for redundant network connectivity between DC and DR site.

3.3.9 The solution should provide a Recovery Point Objective (RPO) – 5 minutes and Recovery Time Objective (RTO) – 4 hours.

3.3.10 SI should compare multiples disaster recovery management tools under following criteria,

(i) Ease of use

(ii) Monitoring capabilities

(iii) Automatic backup of critical data and systems

(iv) Quick disaster recovery with minimal user interaction

(v) Flexible options for recovery

(vi) Recovery point and recovery time objectives

(vii) Compatibility with physical servers

(viii) Options for the backup target

and best fit for the requirement to be selected.

3.3.11 SI needs to advise ECGC for DR Plan and document the same for company with holistic view and focus on recovering the application services and not just servers. The technical recovery plan for each application/ service should be documented in a way that all the activities that need to be performed during recovery should be defined in a sequential manner which may include,

- Design for end-to-end recovery
- Define recovery goals
- Make tasks specific: To make the system up and running, all steps should be predefined
- Guess work should not be done
- Documenting the steps is needed
- Maintain more than one DR recovery paths

3.3.12 DR Plan should cover all details such as physical and logical architecture, dependencies (inter- and intra-application), interface mapping, authentication, etc. Application

dependency matrix, interface diagrams and application to physical/ virtual server mapping to be done in coordination with ECGC/ Application team.

3.3.13 SI needs to work together with ECGC in defining Roles and responsibility clearly while planning for a Disaster Recovery roll-out plan. It should contain a governance structure in the form of a Business Continuity-Committee. The Business Continuity Committee will be responsible for:

(ix) Clarify their roles of all the members of the committee

(x) Oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan

(xi) Provide strategic direction and communicate essential messages

(xii) Approve the results of Business Impact Analysis

(xiii) Review the critical services and products that have been identified

(xiv) Approve the continuity plans and arrangement

(xv) Monitor quality assurance activities

(xvi) Resolve conflicting interests and priorities

3.3.14 The solution should adhere to Insurance Regulatory and Development Authority of India (IRDAI) and Ministry of Electronics and Information Technology (MeitY) regulatory guidelines

3.3.15 SI shall be responsible for,

(xvii) Disaster Recovery Management

(xviii) Program Management for DR

(xix) Integration with Business Continuity from hardware perspective

(xx) Plan Maintenance of DR Site

(xxi) Management Actions (Escalations, Declaration and Orchestration)

(xxii) Assist in defining Application interdependencies working cordially with Application MSP and ECGC officials

(xxiii) Assist Application MSP/ ECGC in Defining sequence of recovery

(xxiv) System Recovery from IT infra perspective

(xxv) DR Testing from infra perspective and assistance to Application team

(xxvi) Compute (servers)

(xxvii) Network and peripheral devices

(xxviii) Storage/ Data

(xxix) DR drill as per regulatory compliances and desired frequency of ECGC

(xxx) System Recovery

3.3.16 The project needs to be rolled out as per the timelines mutually agreed with ECGC and selected bidder.

3.3.17 SI shall be able to provide any additional need of devices/ components listed in BOM on the same price for next 180 days from date of work order.

3.3.18 Bidders shall not quote products, whose End of Sale/ End of Support/ End of Life has been declared by the OEM as on RFP submission date. The devices and hardware provisioned by SI shall be under 5 years warranty support from OEM post deployment.

3.3.19 Successful Bidder should deliver the hardware items as per the BOQ and specifications defined in Annexure - 4A and Annexure - 4B .

3.3.20 SI will be responsible for the requisite coordination with OEM in all regards.

3.3.21 SI will have to coordinate with Application MSP(s) of ECGC for the replication of all the applications working at primary DC.

3.3.22 The selected SI will be required to adhere with detailed SOW with SLAs for SI scope and enter into legal agreement with ECGC.

3.3.23 SI shall ensure dedicated SPOC availability at ECGC – HO, Mumbai during the phase of implementation at desired DR Site.

3.3.24 The indicative scope of work for SI is as below:

(i) Designing optimized solution as per hardware specifications given in the tender document.

(ii) Procurement of Hardware

(iii) Installation of hardware, configuration of devices, policy implementation, integration of devices, etc.

(iv) Provisioning of NTT Data Centre at Bengaluru location as a co-location for deploying the IT infra resources as per the specifications given. Installation, commissioning of Data Centre components for five years including all necessary DR site requirements like power supply, cooling, security etc.

(v) Provisioning any additional resources required for maintenance and management of the DR Site. Bidder shall ensure all required Local Handheld support requirements at ECGC DR Site.

(vi) The SI shall have back-to-back arrangement with Infra OEM (s) to meet infra vertical and horizontal scalability requirement on request of ECGC

(vii) Coordinating with different vendors (new or existing) during DR implementation and DR Drills.

(viii) End-to-end testing of DR equipment.

(ix) Meeting CERT-In security standards as per industry best practices and ECGC's security policies and guidelines.

(x) SI need to inform ECGC about any confirmed breach immediately and within 4 hours for suspected breach from the time of breach discovery.

3.3.25 The work commences from the issue of Purchase Order. The Successful Bidder shall be required to provide acceptance of the Purchase Order within 24-48 hours of issuance of the same.

3.3.26 Project Management

(a) The vendor shall appoint a project manager to the onsite location, who shall be responsible for overall project monitoring and management of Project Team and SLA during implementation.

(b) The onsite PM shall require to submit a project progress report based on the nature of duties being executed at DR Site, frequency of the same can be decided mutually.

(c) Even though no specific SLA shall be applicable, However, continued non-compliance / non-conformity / deviation may result in invocation of bank guarantee and / or termination of contract.

3.4 The bidding documents

3.4.1 Documents constituting the Bid:

The Documents constituting the Bid include:

(i) Eligibility Bid (as per the form provided under Annexure -1)

(ii) Technical Bid Sheet (as per the form provided under Annexure-4 A to B)

(iii) Price/ Financial Bid (as per the form provided under Annexure – 5 A to C)

(iv) All other / supporting documents and Annexures as attached.

Sr.No	Bid Envelop	Refer - Annexure Number
1	Eligibility Bid	• Annexure- 1 • Annexure-2 • Annexure-3 • Annexure-7 • Annexure-9 • Annexure-10 • Annexure-12 • Other supporting document
2	Technical Bid	• Annexure-4 A to B • Other supporting document
3	Commercial Bid	• Annexure – 5 A to C) • Other supporting document
4	Post Awarding of Contract by the successful Bidder	• Annexure-6

The Bidder is expected to examine all instructions, forms, terms and specifications in the Bid Document. Failure to furnish all information required by the Bid Document or to submit a Bid not substantially responsive to the Bid Document in every respect will be at the Bidder's risk and may result in the rejection of the Bid.

3.4.2 Pre-bid Meeting:

The Bidder(s) having any doubt/ queries/ concerns with any clause of this document or selection process shall raise their concern within 7 days of release of RFP Document. ECGC will not be liable to accept or provide any explanation towards any doubt/ concerns later on whatever the same may be.

A pre-bid meeting as per schedule given in the RFP document shall be held where bidder's queries will be discussed.

The bidders attending the pre-bid meeting shall compulsorily inform in advance about name, Designation, contact number (Mobile and Landline) of participants before the pre-bid meeting. Not more than 2 participants will be allowed from each bidder company.

The queries shall be communicated only through the e-mail id provided, it-tender@ecgc.in the format provided in Annexure - 8. ECGC would issue clarifications/ Amendments in writing via e-mail and will become part of RFP.

OEMs are requested not to send individual pre-bid queries, instead approach their SI partners / Prime Bidder in the consortium (as the case may be) to submit the pre-bid queries in consolidated fashion. Further, only bidders who intend to participate in the tender process as SI or Prime Bidder in case of consortium, are expected to participate in Pre-Bid meeting and Pre-Bid stages, keeping in mind the varied requirements which are to be integrated into a single comprehensive solution / bid.

3.5 Preparation of bids

3.5.1 Language of Bid

The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Company and supporting documents and printed literature shall be submitted in English only.

3.5.2 Eligibility and Technical Bids

3.5.2.1 Documents comprising the Eligibility and Technical Bids should contain the following completed forms/ documents in accordance with the clauses in the Bid and duly signed by the authorized representative of the Bidder and stamped with the official stamp of the Bidder (Board resolution authorizing representative to bid and make commitments on behalf of the Bidder to be attached):

a) Eligibility and Technical Bid Forms as per Annexure-1 and Annexure – 4 (A to B)

b) Supporting documents as mentioned in Annexure-1 and Annexure – 4 (A to B)

3.5.2.2 The papers like Forms, supporting documents as mentioned above etc. should be submitted in one lot in one envelope for Eligibility Bid and Technical Bid respectively.

3.5.2.3 Any Eligibility and Technical Bids not conforming to the above list of documents will be rejected.

3.5.2.4 The Eligibility and Technical Bids should NOT contain any price information. Such bid, if received, will be rejected.

3.5.3 Price / Financial Bid

Each Bidder is required to complete a Price/ Financial Bid Envelope, comprising of the Price/ Financial Bid Form as per Annexure – 5 on the letter head of the Bidder.

3.5.4 Bid Form

The Bidder shall include requisite documents wherever mentioned for Eligibility, Technical and Price/ Financial Bids, in three separate sealed envelopes and submit them together to the Company in a single outer envelope. Bids are liable to be rejected if all Bids (Eligibility, Technical Bid and Price/ Financial Bids) are not received together, within the timelines for submission of Bids as per Schedule of Events.

3.5.5 Bid Prices

3.5.5.1 Prices are to be quoted in Indian Rupees only.

3.5.5.2 Prices quoted should be exclusive of all Central / State Government levies, taxes (including Service Tax / GST) which will be deducted at source at applicable rates.

3.5.5.3 Prices quoted by the Bidder shall be fixed during the Bidder's performance of the Contract and shall not be subject to variation on any account, including exchange rate fluctuations, during the validity period of the contract. Taxes / Duties / Levies / Cess etc. levied by Central or State Governments, or Statutory, Quasi-Government Bodies, or Regulators may be charged as per actuals, and are allowed to be varied. A Bid submitted with an adjustable price quotation, other than exceptions specified herein, will be treated as non-responsive and shall be rejected.

3.5.6 Documentary Evidence Establishing Bidder's Eligibility and Qualifications

The documentary evidence of the Bidder's qualifications to perform the Contract in its Bid will be accepted only if it is established that the same are to the Company's satisfaction. Please refer to Annexure-1.

3.5.7 Partial bids

Partial Bids will not be accepted and shall be rejected. Bidder(s) shall have to quote for the entire scope.

3.6 Period of Validity of Bids

3.6.1 Bids shall have the validity period of 90 days from the closing date of submission of bids. Bidders are required to offer 90 days price validity as per Bid Terms. The prices quoted shall remain firm and fixed during the currency of the Purchase order/ Contract unless agreed otherwise by the Company.

3.6.2 In exceptional circumstances, the Company may solicit the Bidder's consent to extension of the period of validity of the Bid on the same terms and conditions. The request and the responses thereto shall be made in writing. At this point, a Bidder may refuse the request without risk of exclusion from any future RFPs or any debarment.

3.6.3 The Company reserves the right to call for fresh quotes at any time during the validity period of the Bid, if considered necessary.

3.7 Format and Signing of Bid

3.7.1 Each Bid shall be in three parts:

Part A – Eligibility Bid

Part B - Technical Bid.

Part C– Price/Financial Bid.

Each part should be in three separate sealed NON-WINDOW envelopes bearing the Bidder's name and address (return address), each super-scribed with "Tender Subject" as well as "Eligibility Bid", "Technical Bid" and "Price/Financial Bid" as the case may be.

3.7.2 The Bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The person or persons signing the Bids shall authenticate all pages of the Bids, except for un-amended printed literature.

3.7.3 Any inter-lineation, erasures or overwriting shall be valid only if they are authenticated by the person signing the Bids. The Company reserves the right to reject bids not conforming to above.

3.7.4 All documents submitted in the context of this RFP Document, whether typed, written in indelible ink, or un-amended printed literature, should be legible / readable. Non-

compliance to this clause shall result in Bid being considered as non-responsive, and shall be rejected at the outset.

3.7.5 The bid shall be in A4 size papers, numbered with index and highlighted with technical specification details. Bids should be spirally bound or fastened securely before submission. Bids submitted in loose sheets shall be disqualified.

3.7.6 ADDITIONAL INFORMATION: Bidder may include additional information which will be essential for better understanding of the proposal. This may include diagrams, excerpts from manuals, or other explanatory documentation, which would clarify and/or substantiate the bid. Any material included here should be specifically referenced elsewhere in the bid.

3.7.7 GLOSSARY: Bidder shall provide a glossary of all abbreviations, acronyms, and technical terms used to describe the services or products proposed. This glossary should be provided even if these terms are described or defined at their first use or elsewhere in the bid response.

3.8 Submission of bids

3.8.1 Sealing and Marking of Bids

3.8.1.1 Each Bid shall be in three parts:

Part A – Eligibility Bid

Part B - Technical Bid.

Part C– Price/Financial Bid.

Each part should be in three separate sealed NON-WINDOW envelopes bearing the Bidder's name and address (return address), each super-scribed with "Tender Subject" as well as "Eligibility Bid", "Technical Bid" and "Price/Financial Bid" as the case may be.

3.8.1.2 The Bidder(s) shall seal the NON-WINDOW envelopes containing one copy of "Eligibility Bid", one copy of "Technical Bid" and one copy of "Price/Financial Bid" separately and all these NON-WINDOW envelopes shall be enclosed and sealed in a single outer NON-WINDOW envelope bearing the Bidder's name and address (return address).

3.8.1.3 The inner envelopes shall be addressed to the Company at the address given for submission of Bids in Section 1 above and marked as described in Clauses above.

3.8.1.4 The outer envelope shall:

a) Be addressed to the Company at the said address given in Section 1.2; and

b) Bear the Project Name

3.8.1.5 All envelopes should indicate the name and address of the Bidder on the cover.

3.8.1.6 If the envelope is not sealed and marked, the Company will assume no responsibility for the Bid's misplacement or its premature opening.

3.9 Deadline for Submission of Bids

3.9.1 Bids must be received by the Company at the address specified in Section 1.2, no later than the date & time specified in the "Schedule of Events" (Section 1.2) in Introduction.

3.9.2 In the event of the specified date for submission of Bids being declared a holiday for the Company, the bids will be received up to the appointed time on the next working day.

3.9.3 The Company may, at its discretion, extend the deadline for submission of Bids by amending the appropriate terms and conditions in the Bid Document, in which case, all rights and obligations of the Company and Bidders previously subject to the deadline will thereafter be subject to the extended deadline, which would also be advised to all the interested Bidders on the Company's website.

3.10 Late Bids:

Any Bid received after the deadline for submission of Bids prescribed, will be rejected.

3.11 Modification and Withdrawal of Bids

3.11.1 The Bidder, if after evincing interest in participating in the bidding process and attending the pre-bid meeting, wishes to withdraw from the bidding process, the Bidder may do so without any penal action including debarment or exclusion from future RFPs / contracts / business, provided the bidder submits its decision to the Company in writing, along with its reasons for the same.

3.11.2 The Bidder may modify or withdraw its Bid after the Bid's submission, provided that written notice of the modification, including substitution or withdrawal of the Bids, is

received by the Company, prior to the deadline prescribed for submission of Bids, the Bidder may do so without any penal action including debarment or exclusion from any future RFPs / contracts / business, provided the Bidder submits its decision to the Company in writing, along with its reasons for the same.

3.11.3 No Bid may be modified after the deadline for submission of Bids.

3.11.4 No Bid may be withdrawn in the interval between the deadline for submission of Bids and the expiration of the period of Bid validity specified by the Bidder on the Bid Form. Withdrawal of a Bid during this interval may result in penal action including debarment or exclusion from any future RFPs / contracts / business.

3.12 Opening and evaluation of bids

3.12.1 Opening of Bids by the Company

3.12.1.1 The Company reserves the right to open the Bids soon after their receipt from all the Bidder(s) without waiting till the last date as specified above and also the right to disqualify any or all Bidder(s) either on the basis of their responses, to all or some of the response sheets, or even any part thereof without assigning any reasons whatsoever.

3.12.1.2 The Company at its discretion and if it considers appropriate may announce the Bidders' names, Bid modifications or withdrawals and the presence or absence of requisite documents and such other details.

3.12.1.3 Bids and modifications sent, if any, that are not opened at Bid Opening shall not be considered further for evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

3.12.2 Preliminary Evaluation

3.12.2.1 The Company will examine the Bids to determine whether they are complete, whether the required formats have been furnished, the documents have been properly signed, and that the Bids are generally in order.

3.12.2.2 Prior to the detailed evaluation, the Company will determine the responsiveness of each Bid to the Bid Document. For purposes of these clauses, a responsive Bid is one, which conforms to all the terms and conditions of the Bid Document without any deviations.

3.12.2.3 The Company's determination of a Bid's responsiveness will be based on the contents of the Bid itself, without recourse to extrinsic evidence.

3.12.2.4 If a Bid is not responsive, it will be rejected by the Company and such a Bid may not subsequently be made responsive by the Bidder by correction of the nonconformity.

3.12.3 Evaluation of Bids

3.12.3.1 Only those Bidders and Bids which have been found to be in conformity of the eligibility terms and conditions during the preliminary evaluation would be taken up by the Company for further detailed evaluation. The Bids which do not qualify the eligibility criteria and all terms during preliminary examination will not be taken up for further evaluation.

3.12.3.2 The Company reserves the right to evaluate the Bids on technical & functional parameters.

3.12.3.3 The scoring sheets will be shared only with interested bidders and those participating in pre-bid meeting.

3.12.3.4 The Eligibility Evaluation will be first carried out as per the criteria given in Annexure-1. The Bidders who score minimum of 70% in this Part (Part-A and Part-B each separately) shall be deemed to be qualified for further evaluation.

3.12.3.5 The Technical Evaluation would be carried out (for vendors who qualified Eligibility evaluation criteria of minimum 70% marks) as per the Technical Evaluation Criteria specified in Annexure – 11 of this RFP. The Bidders meeting technical requirements of Tender and having submitted technical bid as per tender conditions will be evaluated further. The incomplete technical bid may be subject to rejection. However, ECGC at its discretion may call for additional documents/ clarification from all bidders, if required.

3.12.3.6 The Bidders submitting bids in accordance of tender condition and qualifying the Eligibility evaluation criteria will be invited for making presentation before the ECGC Technical Evaluation Committee for this RFP, and will be evaluated as per criteria specified in Technical scoring sheet on overall solution designed and proposed.

3.12.3.7 During evaluation and comparison of Bids, the Company may, at its discretion ask the Bidders for clarification of their bid. The request for clarification shall be in writing

and no change in prices or substance of the Bid shall be sought, offered or permitted. No post Bid clarification at the initiative of the bidder shall be entertained.

3.12.3.8 The minimum qualifying marks for technical bid will be 70% marks.

3.12.4 Evaluation of Price/Financial Bids and Finalization

3.12.4.1 The information provided by the Bidder(s) in response to this RFP Document will become the property of ECGC and will not be returned.

3.12.4.2 The bidders receiving minimum 70% marks in Technical bid will be considered for further evaluation and the Price/Financial bids for these Bidder(s) shall be opened.

3.12.4.3 The Price/ Financial Bid will be scored on a total of 100 as under:

a. Cs = (Cmin / Cb) x 100 where,
b. Cs = Commercial score of the Bidder under consideration
c. Cmin = Lowest Price/ Financial Bid quoted
d. Cb = Price/Financial Bid under consideration

3.12.4.4 Bids will finally be ranked on the basis of combined scores arrived as follows: Weight of 70% to the total technical score (combined score under Part – I and Part – II)

3.12.4.5 Weight of 30% to the commercial score

a. Combined Technical and Commercial Score, calculated up to two decimal points, will be as under:
b. Bs = (0.7) * Ts + (0.3) * Cs
c. Where,
d. Bs = overall combined score of Bidder under consideration
e. Ts = Technical score of the Bidder under consideration
f. Cs = Commercial score of the Bidder under consideration
    i. Company may waive off any minor infirmity or non-conformity or irregularity in a Bid, which does not constitute a material deviation, provided such a waiving does not prejudice or affect the relative ranking of any Bidder.
    ii. Company reserves the right to reject any or all incomplete Bids.
    iii. Bidder(s) bidding in the process shall give as a part of the Bidding documents a statement on their letter head, as per the format provided under Annexure - 3, that they have no objection with any clause of the Tender Document.

3.12.5 Contacting the Company

3.12.5.1 No Bidder shall contact the Company on any matter relating to its Bid, from the time of opening of Price/Financial Bid to the time the Contract is awarded.

3.12.5.2 Any effort by a Bidder to influence the Company in its decisions on Bid evaluation, Bid comparison or contract award may result in the rejection of the Bidder's Bid and its barring from any future RFPs / contracts / business with ECGC.

3.12.6 Award Criteria

The Bidder that gets the highest combined technical and commercial score shall be awarded the Contract. ECGC Ltd. will notify the successful Bidder in writing, by letter or by e-mail, that its Bid has been accepted. The notification of award will constitute the formation of the offer to contract. The selected Bidder should convey acceptance of the award of contract by returning duly signed and stamped duplicate copy of the award letter within seven working days of receipt of the communication. In case of a tie, the Bid having higher score in technical evaluation will be considered the best bid value. In case the selected Bidder fails to accept the award then the Bidder securing the next highest combined score among the Bidder(s) (other than the Bidder who has failed to accept the award) will be considered for the award and so on. The successful Bidder will have to submit the Performance Bank Guarantee and execute a Service agreement within 15 working days of the award of Contract, which will be valid for the tenure as mentioned in this RFP Document

3.12.7 Company's Right to Accept Any Bid and to reject any or All Bids:

3.12.7.1 The Company reserves the right to accept or reject any Bid or to cancel the Bidding process and reject all Bids at any time prior to contract award, without incurring any liability to the affected Bidder or Bidder(s) or any obligation to inform the affected Bidder or Bidders of the grounds for the Company's action.

3.12.7.2 All decisions taken by the Company are binding and final.

3.12.8 Performance Bank Guarantee

3.12.8.1 The successful Bidder (hereinafter referred to as the 'Vendor') shall be required to submit a Performance Bank Guarantee ("PBG") as per pro-forma attached as Annexure - 6 for a value equal to 10% of the Contract value (inclusive of applicable taxes) or equal to two quarters payment amount, valid for the period of the Contract (plus additional 8 weeks for claim period) from the date of satisfactory acceptance/ sign off by ECGC.

3.12.8.2 The PBG of correct value and validity period as mentioned above must be submitted within two weeks from the date of acceptance of the Letter of Award.

3.12.8.3 In case the contract period is extended beyond six months due to nature of work, the PBG shall have to be extended / renewed / re-issued for the new / extended contract period, including the claim period. The Vendor to make provisions for submission of extended PBG at least two weeks before the expiry of the original term of PBG in such case.

3.12.8.4 PBG shall be forfeited if the services are terminated abruptly by the Vendor or for any deviation by the Vendor from the terms of the Contract by way of which the Company can decide to forfeit the PBG. Further, unpaid charges, if any, will also not be paid in these circumstances. In case of no punitive action against the Vendor, the PBG will be returned after the 8 weeks from the satisfactory acceptance/ signoff by ECGC or on settlement of any claim against the Vendor, whichever is later.

3.12.9 Earnest Money Deposit

Earnest Money Deposit (EMD) of Rs. 5,00,000 (Rupees Five lakh only) is required to be submitted preferably by NEFT. EMD can also be paid by Demand Draft/ Bankers Cheque by the vendors along with the tender. The Demand Draft/ Bankers Cheque must be issued in favor of '**ECGC Limited'**, payable at Mumbai.

Bank details for submission of the EMD are as below:

Bank Name:	IDBI Bank Ltd.
Bank Account Number:	V003423133000003

IFSC Code:	IBKL0000004
A/c Name / Beneficiary Name:	ECGC of India Ltd
Bank Branch:	Nariman Point, Mumbai
Bank Branch Address:	224-A, MITTAL TOWER, A WING, NARIMAN POINT, MUMBAI -21
MICR Code	400259002
Narration	From – Name of Company

The transfer of the EMD amount needs to be completed along with submission of bid documents as per RFP Schedule of events 1.2 It is the bidder's responsibility to ensure timely transfer of the EMD.

If the EMD is received after the designated date and time, the Company, at its discretion may reject the bid.

EMD of unsuccessful Bidders shall be refunded within 30 days from the final result of the bidding process and declaration of the Successful Bidder.

EMD of successful bidder shall be refunded within 30 days post receipt of PBG without any interest.

Under any circumstances, ECGC Limited will not be liable to pay any interest on the EMD. Offers made without the Earnest money deposit will be rejected.

The bidder needs to ensure that the correct amount is calculated and reflected in the EMD. Any arithmetic calculation errors in the EMD will lead to disqualification of the bidder.

The amount of Earnest money deposit would be forfeited in the following scenarios:

a. In case the Bidder withdraws the bid prior to validity period of the bid without providing any satisfactory reason;

b. In case the successful Bidder fails to accept and sign the contract as specified in this document without any satisfactory reason; or

c. In case the successful Bidder fails to provide the performance bank guarantee within 30 working days from the date of issuance of PO, without any satisfactory reason.

Section - 4

4.1 TERMS AND CONDITIONS OF CONTRACT (TCC)

4.1.1 Definitions:

In this Contract, the following terms shall be interpreted as indicated:

4.1.1.1 "The Company" means ECGC Limited

4.1.1.2 "Vendor" is the successful Bidder whose Bid has been accepted and gets the highest combined technical and commercial score and to whom notification of award has been given by the Company

4.1.1.3 "The Services" means the scope of services which the Vendor is required to provide ECGC under the Contract

4.1.1.4 "The Contract" means the agreement entered into between ECGC and the Vendor, and signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein

4.1.1.5 "The Contract Price" means the price payable to the Vendor under the Contract for the full and proper performance of its contractual obligations

4.1.1.6 "TCC" means the Terms and Conditions of Contract

4.1.1.7 "The Project" means "APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED"

4.1.1.8 "The Project Site" means designated locations of ECGC Limited as may be specified in Purchase Order / Contract

4.1.2 Scope of Work

As described in clause 3.3 of The Request for Proposal (RFP) Document.

4.1.3 Payments

4.1.3.1 Payment shall be made in Indian Rupees.

4.1.3.2 Payment shall be made via electronic fund transfer only to the bank account specified, as per the form provided under Annexure -2, in the RFP response.

4.1.3.3 No payment shall be made in advance on award of the contract.

4.1.3.4 Payments shall be made only on receipt of invoice from the Vendor, after completion of the scope of work to the satisfaction of ECGC Limited, on milestone basis.

4.1.3.5 All payments shall be subject to TDS and any other taxes as per the tax rules prevalent at the time of payment.

4.1.3.6 It may be noted that ECGC will not pay any amount / expenses / charges/ fees / travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses other than the agreed amount as per the purchase order / contract.

4.1.3.7 Any decrease in taxes must be passed on to ECGC.

Payment Terms:

4.1.3.8 The payment will be done on OPEX model as quarterly advance for the delivered services and goods.

4.1.3.9 GST to be calculated on actuals at the time of billing.

4.1.4 Liquidated Damages

Liquidated Damages, wherever referred under this RFP/ Agreement, shall mean and refer to the damages, not in the nature of penalty, which the Vendor agrees to pay in the event of delay in delivery of services, installation, commissioning, breach of contract etc. as the case may be.

The date of delivery of the services, Installation and/or Commissioning as stipulated and accepted by the Vendor should be deemed to be the essence of the contract and delivery must be completed not later than the dates specified therein. Extension will not be given except in exceptional circumstances subject to conditions as enumerated in the contract/ tender including levying of Liquidated Damages as specified below.

Liquidated Damages is not applicable for reasons attributable to ECGC and/or Force Majeure. However, it is the responsibility/ onus of the Vendor to prove that the delay is attributed to the ECGC and/or Force Majeure. The vendor shall submit the proof that the delay is attributed to the ECGC and/or Force Majeure along with the bills requesting payment.

While granting extension of delivery period, the liquidated damages shall be levied as follows:

- if the Vendor/ appointed SI fails to install and commissioning the project within the stipulated time, ECGC shall be entitled to recover Liquidated Damages at 2% of the value of the purchase order for each week of delay or part thereof for a period up to 5 (five) weeks. In cases where the delay affects installation/ commissioning of only a

part of the project and part of the equipment is already in commercial use, then in such cases, Liquidated Damages shall be levied on the affected part of the project.

- Project extension period beyond 5 (five) weeks would not be allowed. The extension beyond 5 weeks may be decided in most exceptional circumstances on case-to-case basis, by the competent authority of ECGC, stating reasons and justifications for grant of extension.

The total value of the liquidated damages as per above shall be limited to a maximum of 10 percent of the total value of the purchase order. Notwithstanding anything contained in this Agreement or any other agreement between the parties, ECGC may, without prejudice to its right to effect recovery by any other method, deduct the amount of Liquidated Damages from any money belonging to the Vendor in its hand in relation to this or any other contract between the parties (which includes ECGC's right to claim such amount against invoices raised by the Vendor or Bank Guarantees submitted by the Vendor under this Contract or any other contract) or which may become due to the Vendor. Any such recovery of Liquidated Damages shall not in any way relieve the Vendor from any of its obligations to complete the Works or from any other obligation and liabilities under the Contract.

To facilitate recovery of Liquidated Damages from the invoices raised by the Vendor, the Credit Note shall be issued by the supplier, failing which the ECGC shall adjust the amount to be recovered from the pending payments by issuing an invoice/ debit note for the corresponding amount, at the risk and cost to the Vendor including applicable GST, interest and penalty, if any.

4.1.5 Service Delivery Location

The entire scope of work as mentioned above will be required to be delivered at third party NTT DR- Data Centre, Bengaluru. However, the Vendor's team may be required to travel to ECGC's Registered Office in Mumbai or IT department at BKC or other nearby locations in Mumbai, for meetings with / discussions with / presentations to ECGC's Senior Management. The Team would be required to travel and / or be posted at ECGC's Data

Centre Site in Bengaluru and Mumbai for work-related matters. The Team may also be required to travel for meetings with / discussions with / presentations to the Technical Advisory Committee (TAC) of ECGC and / or to the Board of Directors of ECGC, and for vendor selection meetings, and / or Data Centre visits as required for RFP evaluation, etc.

4.1.6 Service Delivery Period

The Vendor is expected to draw out and present the overall timeline for service delivery in accordance with milestones presented by the Vendor in the RFP response and the Solution Presentation as described in Section 1 of the RFP Document. The SI will be required to install, configure, commission and ensure operation of DR environment by **December - 2024.**

These will form the basis of delivery timelines. The exact specifications of the timelines and consequent milestone-based payment schedule shall be mutually agreed upon with the Vendor, subject to no advance payments. ECGC Ltd reserves the right to grant an extension, and / or cancel the order, and / or invoke the PBG, and/or take appropriate legal action in the event of any breach of contract.

4.1.7 Termination

ECGC may terminate the Contract with at least 15 days prior written notice to the Vendor on account of any material breaches committed by the Vendor in breach of its obligations under the Contract.

ECGC shall not be obligated to pay the Vendor for any such terminated services performed or expenses incurred after the effective date of such termination.

4.1.8 Indemnity

The Vendor shall indemnify, protect and save ECGC against all claims, losses, costs, damages, expenses, action suits and other proceedings resulting from any infringements in respect of all hardware, software, and services being utilized by the Team / resources, except for those explicitly provided by / authorized by ECGC.

4.1.9 Arbitration

In the event of a dispute or difference of any nature whatsoever between ECGC and the Vendor during the course of the Contract, the same shall be referred to arbitration comprising of a sole arbitrator. The Arbitration shall be carried out in English language at ECGC office with address as mentioned in schedule of events 1.1 and as per the provisions of the Arbitration and Conciliation Act, 1996 (as amended from time to time). The seat of Arbitration shall be Mumbai.

4.1.10 Governing Law and Jurisdiction

The High Court of Bombay shall alone have jurisdiction for the purposes of adjudication of any dispute of differences whatsoever in respect of or relating to or arising out of or in any way touching the works awarded or the terms and conditions of the Contract.

4.1.11 Survival

The termination of the Contract shall not affect the rights of and or obligations of the Vendor which arose prior to the termination.

4.1.12 Working on ECGC's Holiday

Request for permission for working on Saturday / Sunday / holidays if required, should be submitted 3 working days prior to the date of holiday, to respective locations head. The Vendor should provide the visiting Team member's details in advance to respective offices. The Team Member shall visit at the scheduled date and time and show his identity card/ permission letter when asked for.

4.1.13 Force Majeure

Notwithstanding the provisions of TCC, the Vendor shall not be liable for forfeiture of its Performance Bank Guarantee, liquidated damages, or termination for default, if and to the extent, that, the delay in performance, or other failure to perform its obligations under the Contract, is the result of an event of Force Majeure.

For purposes of this clause, "Force Majeure" means an event beyond the control of the Vendor and not involving the Vendor's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Company in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

If a Force Majeure situation arises, the Vendor shall promptly notify the Company in writing of such condition and the cause thereof. Unless otherwise directed by the Company in writing, the Vendor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

4.1.14 Entire Agreement

It is expressly agreed between the parties that the Contract, The Request for Proposal (RFP) Document, any addendum or corrigendum issued thereafter and the completed Annexures thereto constitutes the Entire Agreement between the Parties.

4.1.15 Rights of the Company:

4.1.15.1 ECGC does not bind itself to accept the lowest quotation and reserves the right to reject any or all the quotations received, without assigning any reason thereof.

4.1.15.2 While processing the Bids, ECGC further reserves the right to delete or reduce any item or section contained in the Tender Document or in the Scope of Work without assigning any reason thereof.

4.1.16 Royalties and Patents

Any royalties or patents or the charges for the use or infringement thereof that may be involved in the contract shall be included in the price. Vendor shall protect the Company against any claims thereof.

4.1.17 Intellectual Property Right (IPR)

The Vendor shall provide Reports, Documents and all other relevant materials, artifacts etc. during the Assignments to ECGC Ltd. and ECGC Ltd. shall own all IPRs in such Reports, Documents and all other relevant materials, artifacts etc. All documents related to such shall be treated as confidential information by the Bidder. The ownership of all IPR rights in any and all documents, artifacts, etc. (including all material) made during the Term for Assignment under this Agreement will lie with ECGC Ltd.

4.1.18 Representation and Warranties

Vendor servicing the Company should comply with the Company's IS Security policies in key concern areas relevant to the activity, the broad areas are:

i. Responsibilities for data and application privacy and confidentiality.

ii. Responsibilities on system and software access controls and administration.

iii. Custodial responsibilities for data, software, hardware and other assets of Company being managed by or assigned to vendor.

iv. Physical security of the Services / Equipment provided by the vendor.

v. The Vendor has necessary expertise to provide the Services and is duly authorized to enter into this Agreement and to perform the Services to the best of its abilities in a professional workmanlike manner and deliver the services to the Company in accordance with scope of work and is under no contractual and/or legal restriction which may in any manner interfere in the performance or delivery of Services

vi. It is authorized to execute and implement the Agreement and discharge its obligations thereunder and in terms of the applicable laws and regulations.

vii. The performance of its obligations as per the Agreement does not and shall not violate or conflict in any manner with any duty or obligation owed to any third party.

Vendor shall also be required to comply with statutory and regulatory requirements as imposed by various statutes, labour laws, local body rules, state and central Government Body statutes, and any other regulatory requirements applicable on the Vendor, and shall produce the same for records of ECGC Limited and / or its Auditors and / or its regulator.

4.1.19 SLA

Sr.No	Activity	Acceptance (YES/NO)	Penalty Terms
1	24 x 7 x 365 online support coverage for hardware and Software calls logged.		Rs. 10,000/- per day, maximum up to 10% of total PO value
2	Successful bidder must ensure direct OEM support (24 x 7 x 365) for any hardware and software issue and it is the responsibility of the bidder to ensure that ECGC gets all necessary support from the OEM team to address technical issues (if required) for timely resolution.		Rs. 10,000/- per day, maximum up to 10% of total PO value
3	SLA during warranty for software issues: Response time of 4 hours from the time of logging the call		Rs. 10,000/- per day, maximum up to 10% of total PO value
4	Delay in Project Execution:		Delay in Project Execution shall attract penalty calculated @1% of total PO value per day of delay, maximum up to 10% of total PO value, beyond which ECGC reserves the right to get the project completed by the third party at the cost and expenses of the successful bidder
5	Uptime commitment of 99.9% calculated on a yearly basis for Datacenter		Rs. 10,000/- per hour or part there of additional cumulative downtime per year, maximum up to 10% of total PO value

*Please Note: Warranty start date shall be from the product delivery and installation date for the 5 years.

****

Annexure – 1: Eligibility Criteria & Specifications

(A) SYSTEM INTEGRATOR'S ELIGIBILITY CRITERIA:

1	Name of the company			
2	Legal Status (eg. Proprietorship, partnership, limited liability partnership, Company etc. (attach a copy of certificate of incorporation)	<Certified copy of the Certificate of incorporation issued by the Registrar of Companies / Partnership Deed>		
3	Registered Physical Address			
4	Correspondence Address			
5	Business profile of the company (attach a separate write-up or brochure regarding business activities of the company)			
6	Incorporation Date			
7	Board of Directors / Management / Promoters / Partners	(i)		
		(ii)		
		(iii)		
		(iv)		
		(v)		
8	Contact Person Details (Name, Landline and mobile Number, e-mail id)			
9	e-mail id of the bidder			
10	PAN of the bidder	<copy required>		
11	TIN of the bidder	<copy required>		
12	GST Registration No.	<copy required>		
13	Any other statutory license required to operate the business in India, PF, ESIC etc. as applicable from time to time with respect to this Contract.			
14	Details of managerial, supervisory, and other staff available	< Undertaking of the organization confirming the availability of the adequate manpower of requisite qualification and experience for deployment in ECGC. >		

15	Power of Attorney/authorization for signing the bid documents, if applicable.				
16	Copy of entire tender document duly signed and stamped on each page as a token of acceptance is to be attached.				
17	The Bidder should not have been black listed by any Govt. Financial Institutions / Banks / Government / Semi-Government departments in India.	< A self-declaration by the Bidder on its letter head.>			
18	The firm or its affiliates should have never been blacklisted / barred / disqualified by any regulator / statutory body/ judicial or any other authority.	< A self-declaration by the Bidder on its letter head.>			
19	The Bidder's Firm should not be owned or controlled by any Director or Employee of ECGC Ltd.	< A self-declaration by the Bidder on its letter head.>			
20	Should have expertise in all infrastructure / Application Development / Database support.	<Please attach evidences, and use separate sheets as necessary>			
21	Bidders should be a profitable company for last 10 years.	<Please attach evidences>			
22	Bidder must propose end to end solution on Opex Model which should be transferred in ECGC name at the end of 5 years with no additional cost. (Past experience of providing IAAS of single order value of 10 crore or more)				
23	Bidders Company should have at least 25-35 years of existence in India.	<Please attach evidences >			Maximum Marks 10
	Company with 25-30 years of experience			3	
	Company with 31-35 years of experience			7	
	Company with 35+ years of experience			10	
24	Bidders should be at least 100-150 People Company.	<Please attach evidences>			Maximum Marks 10
	100 People Company			3	
	101-150 People Company			7	

	150+ People Company		10	
25	Bidder's average turnover during last 2 years ending 31st March at least 50,00,00,000/ and should provide Audited / Certified Balance sheet, Profit & Loss account for past 2 years ending 31st March 2024	< IT returns acknowledgments and / or Audited Financial Statements / statements certified by Chartered Accountants to be provided for last two financial years ended on 31.03.2024 >		Maximum Marks 10
	Turnover between 50,00,00,000/- to 60,00,00,000/-		5	
	Turnover between 60,00,00,001/- to 90,00,00,000/-		7	
	Turnover above 90,00,00,000/- (90 Cr)		10	
26	Bidder should be profitable company with net profit of at least 5% in last 2 years.	< IT returns acknowledgments and / or Audited Financial Statements / statements certified by Chartered Accountants to be provided for last two financial years ended on 31.03.2023 >		Maximum Marks 10
	Company with net profit of 5%		5	
	Company with net profit of 6 to 7%		7	
	Company with net profit of 8 to 10%		10	
27	Bidder should have direct presence for support in at least all the Four metro cities of India for related work.	Office Address's to be provided		Maximum Marks 10
	Company with presence in four locations		3	
	Company with presence in five locations		7	
	Company with presence in Six location		10	
28	Bidders should provide 3 customer references (Infra Implementation and setting up Datacenter either at third party Data Centre in co-location or on-premise)	<Please attach evidences>	5	Maximum Marks 5
29	The DR Service Provider should be a government organization/ Public sector unit/ Partnership firm / Public Limited Company/ Private Limited	<Please attach evidences>		Maximum Marks 5

	Company having its Registered Office in India since last 5-10 years as on 31/03/2024			
	between 5- 10 Years		3	
	10+ Years		5	
30	Bidder should have experience in IT infrastructure and Application (ERP/CRM) development and maintenance and 3-8 customer references for Managed Services for Infra and Application support.	<Please attach evidences, order value, copies>		Maximum Marks 10
	Up to 2 customer reference		1	
	3-5 Customer reference for Application and Infra support		5	
	6-8 Customer reference for Application and Infra support		8	
	8+ Customer reference for Application and Infra support		10	
31	Bidder should have successfully done at least one implementation of Similar solution on turnkey basis in last 2 years.	<Please attach a separate sheet, if required. (Give scope of work for each assignment) with letters of award/ completion certificate from the respective organizations supporting the same.>		Maximum Marks 10
	Bidder with 1-2 Similar Solution implementations		1	
	Bidder with 3-4 Similar Solution implementations		2	
	Bidder with 4+ Similar Solution implementations		5	
32	Bidder Should Have head office in Mumbai and fully operational office at Bengaluru	<Please attach evidences>	5	Maximum Marks 5
33	The Bidder should submit a certificate issued from each OEM stating that the Bidder is an authorized entity to supply, install, commission, test and support the proposed product at ECGC	<Please attach evidences, and use separate sheets as necessary>	5	Maximum Marks 5

34	Bidder should produce an Authorization Letter in favor of ECGC with reference to this RFP assuring full guarantee and warranty obligations for a MINIMUM period of Five years from the date of PO released.	<Please attach evidences, and use separate sheets as necessary>		Maximum Marks 2
35	Number of professional staff who are proposed to be associated for executing the assignment with names including that of the Team Leader. The Team Leader, once assigned to ECGC Limited, should not be replaced except with the consent from ECGC Limited in writing.	< Resume of the identified team persons in the format enclosed as CV format to this document (Annexure – 7). >		Maximum Marks 3
36	Bidder should have minimum 5 years of experience of hosting data centers Services at NTT and Should be MSP partner with NTT			Maximum Marks 5

Technical Specification of DR: Quantity

1	Rack server compatible with Vmware as virtualisation	Application Server	18	Servers with configuration of Rack mountable with 2 x 24 core per Processor, Minimum RAM of 512 GB and 5 x 1.92 TB All flash Storage Network 1-10 G,1-10G SFP, 24 GE RJ45 Network 1-10G 1-10G SFP, Minimum 24 port Switch with 24 x 10G Short Range SFP+ populated Minimum 2 x 10Gb / 40 G or higher QSFP+/ Built in Monitoring software inter site VMware Enterprise licenses.
		Database Server	2	
		DMS Server	2	
		DRM Server	1	
		Monitoring Server	1	
2	Storage	150 TB usable capacity	1	All flash Storage Box will be recommended for optimum performance with Ransomware Grantee
3	Layer 3 Switch	Networking Device	1	

4	Distribution Switch (TOR)	Networking Device	2	
5	SDWAN Router		1	Existing ECGC ISP will Manage this
6	IPS/IDS	Security Device	1	Palo alto Next Generation firewall
7	UTM	Security Device	1	Fortinet Firewall (As this is deployed in DC)
8	WAF + GSLB + SLB	Security Device	1	F5 Load balancer (As this is deployed in DC)
9	Replication Software between DC and DR	Replication Software	1	Veeam/Zerto/VMWare replication (SRM)
10	Server Security	Deep security	100	Trend Micro (As this is deployed in DC)
11	DAM	Imperva	6	Imperva (As this is deployed in DC)

(B) OEM'S ELIGIBILITY CRITERIA as per technical specifications of servers and storage given below:

Sr. No.	Description	Details	Score	Maximum Score
		<Please attach evidences>		
1	OEM Should be in the leaders list of the acceptable industry reports.			
2	Server and Storage should be managed from one central console (Intersight).		5	5
3	Proposed OEM should have experience of minimum 5 years			Maximum Marks 15
	5 or less years		5	
	6-7 Years		7	
	8-10 years		15	
3	The Server & Storage solution should support scaling and should be from the independent vendors.		10	10
4	The network switch should support QoS to streamline East-West network traffic to improve traffic filtering, segmentation and performance.		10	10
5	The proposed storage system should have minimum, 4 numbers of 12Gbs or higher backend SAS ports, 8x16G FC ports/10G ports across dual controllers		10	10
6	Proposed Server and storage should be centrally managed by Intersight Management tool (already deployed in ECGC environment)		15	15
7	Each Server should be configured with 2 * 480GB using latest M.2 SSD Drives.		5	5
8	Support for integration with Microsoft System Center and PowerShell toolkit		5	5
9	Proposed Storage should be 150 TB usable after configuring RAID 6 or equivalent with NLSAS drives		5	5
10	Server should support Up to 24 front facing SFF SAS/SATA HDDs or SAS/SATA SSDs or NVMe SSDs.		5	5

11	Storage Proposed should be having all flash and should be configured with RAID 5.		5	5
12	Offered Storage system shall be supplied with required software/services to ensure seamless data replication from existing E2800 and vice versa.		10	10
		Total		100

Technical Specifications of the Servers:

S.No	Description	Specification	Compliance (Yes/ No)
1	Form factor	Rack	
2	Size (RU)	1/2	
3	Processor Make	Intel CISCO (X86)	
4	Number of sockets available on chipset	2	
5	Number of sockets populated with processor	2	
6	Number of core per Processor	24	
7	Processor Configuration	Up to two Latest Intel® Xeon® Scalable Gold Sapphire Rapids processors, (To be populated with dual processor each having min 2.6 GHz clock speed, 60MB Cache)	
8	Chipset compatible with CPU	Intel 621 or Higher	
9	Availability of Co-Processor	No	
10	PCI Slots (Express Gen 3.0)	2	
11	Type of RAM	DDR-4	
12	RAM Size (GB)	512	
13	RAM upgradable upto (TB)	Upgradable to 3TB	
14	DIMM Slots (No.)	24	
15	Type of Hard Disk Drive	SSD	
16	Hard disk drive Capacity (GB)	8 *960 GB	
17	I/O Slots	At least 6 * PCIe Gen4 Slots and 2 Gen 5 slots	
18	Video Controller (support VGA or above resolution)	Yes	
19	Populated Bays (min. 2 or more internal hot plug)	Min. 8	

20	USB Ports (version 2.0/3.0)	2	
21	Redundant Power Supply	Redundant platinum grade Power Supplies	
22	Redundant Fan	redundant hot plug system fans	
23	Total No of Ethernet Ports	3x1G, 4x25G SFP	
24	Server scalability to be achieved within the box without adding nodes	Yes	
25	RoHS Compliance	Yes	
26	Max. power consumption of the system (Watt)	800	
27	Certification and Compliance	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Cent OS	
28	On Site OEM Warranty (years)	Server Warranty (Hardware) includes with 5-year comprehensive warranty with no additional cost for change, replacement of parts, labour, consumable, shipment, insurance etc. 24x7 support with 4 hours of response time & 48-hour resolution time.	
29	Certification/Compliance	Supports & Compatible with offered Solution	
30	Support for high availability clustering and virtualization	Yes	

……

Signature of the authorized Signatory of Bidder

(Seal)

Name:

Designation:

Contact No (Mobile)

Annexure – 2: Bank Details of Bidder

Sr No	Description	Details
1	Name of the Bank	
2	Address of the Bank	
3	Bank Branch IFSC Code	
4	Bank Account Number	
5	Type of Account	

……

Signature of the authorized Signatory of Bidder

(Seal)

Name:

Designation:

Contact No (Mobile)

Email Id

Annexure – 3: Acknowledgement

Date:

To,

Deputy General Manager

Information Technology Division,

ECGC Limited,

Dear Sir/Madam,

Subject: APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED

1. Having examined the Request for Proposal Document including Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide services in accordance with the scope of work as stated in the RFP Document within the cost stated in the Bid.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this RFP.
3. We certify that we have provided all the information requested by ECGC in the requested format. We also understand that ECGC has the right to reject this Bid if ECGC finds that the required information is not provided or is provided in a different format not suitable for evaluation process for any other reason as it deems fit. ECGC's decision shall be final and binding on us.
4. We agree that ECGC reserves the right to amend, rescind or reissue this RFP Document and all amendments any time during the tendering.
5. We agree that we have no objection with any of the clauses and bidding process of this Tender Document.

……

Signature of the authorized Signatory of

(Seal)

Name:

Designation:

Contact No (Mobile): Email ID:

Annexure – 4A: Technical Specifications for Servers and Storage

(1.) Servers:

S.NO	Details	Complied (Yes/NO)
1	Max. 2U Rack Mounted	
2	Up to two Latest Intel® Xeon®Scalable Gold Sapphire Rapids processors, (To be populated with dual processor each having min 24 Cores 2.6 GHz clock speed, 60MB Cache)	
3	32 DDR5 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 4800MT/s and scalable up to 8TB of Memory	
4	512GB 4800 Mhz memory should be offered in each node. Memory should be offered in a balanced configuration so that maximum memory channels can be utilized.	
5	Server should support Up to 24 front facing SFF SAS/SATA HDDs or SAS/SATA SSDs or NVMe SSDs.	
6	Each Server should be configured with 2 * 480GB using latest M.2 SSD Drives.	
7	12Gbps SAS RAID controller with 4GB Cache supporting RAID 0,1, 5, 6,10, 50, 60 supporting capacity drives configured in system.	
8	At least 6 * PCIe Gen4 Slots and 2 Gen 5 slots	
9	One Dual port 32G FC	
10	Min 2 x 10G BaseT and 2 * Quad Port 10/25G Ethernet Ports.	
11	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Cent OS	
12	Platinum rated redundant Power Supply	
13	Support for integration with Microsoft System Center and PowerShell toolkit	
14	Integrated diagnostics and Power monitoring and reporting, Dynamic Power capping.	
15	System should support multiple management interface like Web UI, CLI and XML API. Management solution should be able to manage different form factor hardware and provide single console.	
	Real-time out-of-band hardware performance monitoring & alerting.	
	Remote Power On, Off and reset from Web UI, XML API and KVM.	
	The management tool should be able to provide global resource pooling and policy management to enable policy-based automation and capacity planning	

	Zero-touch repository manager and self-updating firmware system, Automated hardware configuration and Operating System deployment to multiple servers	
	Virtual IO management / stateless computing	
	The server should support industry standard management protocols like IPMI v2 and SNMP v3 and Redfish v1.01	
	Console record and play, Virtual Media, LDAP & HTML5 remote control.	
	The management software should participate in server provisioning, device discovery, inventory, diagnostics, monitoring, fault detection, auditing, and statistics collection.	
	Server management system should provide an alert in case the system is not part of OEM Hardware Compatibility list & should provide anti counterfeit.	
	The proposed management solution should provide proactive security & software advisory alerts and should outline the fixes required to address the issues.	
	The proposed management solution should analyze current configurations & identify potential issues due to driver & firmware incompatibility	
	The proposed management solution should provide policy control to prevent drift of server configurations.	
	The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure. With option to create unique dashboards for individual users. The user should have flexibility to select names for dashboards and widgets (ex: - health, utilization etc.).	
16	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber-attacks	
	Should protect against firmware which executes before the OS boots	
	Hardware based Root of Trust	
	Signed firmware updates	
	Secure default passwords	
	Secure alerting	
	Automatic BIOS recovery	
	Rapid OS recovery	
	Chassis Intrusion Detection	
	System Lockdown	
	System Drift Detection	
	Configuration upgrades should be only with cryptographically signed firmware and software	
17	The Hardware should be IPV 6 Compliant ready	

18	5 years On-site comprehensive warranty with 24x7x365 hardware support.	

(2.) Storage:

S.NO	Details	Complied (Yes/NO)
1	The Storage Solution should be based on dual controllers in active-active mode configured in a NSPOF offering data assurance as per T10-PI standard and End-to-End Data Protection.	
2	The system should have minimum 64 GB cache memory across the two controllers with an ability to protect data on cache if there is a controller failure or power outage. The cache on the storage should have 72hrs or more battery backup (OR) should have destaging capabilty to either flash/disk. The system should also offer extended cache based on SSD.	
4	The system must support intermixing of SSD, SAS and NL-SAS/SATA drives to meet the capacity and performance requirements of the applications.	
5	The storage should be configured with FCP & iSCSI protocols. Any hardware/software required for this functionality shall be supplied along with it in No Single Point of Failure mode.	
6	Should support various RAID levels 0, 10, 5, 6	
7	150 TB usable after configuring RAID 6 or equivalent with NLSAS drives	
8	The system must support intermixing of SSD, SAS and NL-SAS dual ported drives to meet the capacity and performance requirements of the applications. The system must support a minimum of a 96 disks per two controllers for scalability purpose.	
9	The proposed storage system should have minimum, 4 numbers of 12Gbs or higher backend SAS ports, 8x16G FC ports/10G ports across dual controllers	
10	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided and installed by the vendor.	
11	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.	
	The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.	
	The proposed storage system should be configured to provide data protection against two simultaneous drive failures.	
	Proposed system should have high reliability and 99.9999% (six nines) of availability	
	Storage system should support RAID level distributing data across multiple Disk to ensure faster rebuild time.	
	Storage system should allow changing of cache block size non-disruptively for defined RAID group levels to meet various kind of workload.	

	System should have redundant hot swappable components like controllers, disks, power supplies, fans etc.	
12	The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 512 snapshots per system. The license proposed should be for the complete supported capacity of the system.	
13	The system should support instant creation of clones of active data	
14	Easy to use GUI based administration interface for configuration, storage management and performance analysis tools	
15	Support for industry-leading Operating System platforms including: LINUX, Microsoft Windows, HP-UX, SUN Solaris, IBM-AIX, etc. It shall support connecting hosts over iSCSI or FC and shall be supplied with any Multipathing software, if required, with the solution.	
16	The Hardware and software quoted should have 5 years support along with upgrade and updates.	
17	Offered Storage system shall be supplied with required software/services to ensure seamless data replication from existing E2800 and vice versa.	

(3.) Virtualization:

S.NO	Specifications	Compliance (Y/N)
1	The solution should have log analytics available in one single management window to make troubleshooting easier. Should provide a single location to collect, store, and analyse unstructured data from OS, VMs, apps, servers, storage, network and security devices, containers, Kubernetes etc. at scale. Should provide intuitive dashboard and should allow IT teams to search for certain event patterns & types for troubleshooting.	
2	The Solution should have Integrated log management and operation management, in order to better co-relate incidents happening and Should be able to perform Root Cause Analysis and corelation charts to detect deep issues with individual virtual machine, including Automated and Guided Remediations	
3	Should be able to add all types of structured and unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand with long term Log retention and Log archival for future access.	
4	The solution should provide automatic private cloud metering and consumption analysis.	
5	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management, troubleshooting workbench with compliance etc.	

6	The solution should provide capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	
7	Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.	
8	The solution should provide out of the box capacity analytics and modelling, with granularity ranging from entire datacentre to cluster to individual host and virtual machine level.	
9	Single view of all virtual machines, allow Monitoring of system availability and performance and automated notifications with alerts. Monitor, analyse virtual machines, server utilization availability with detailed predict analysis of what's-if Scenario hardware procurement, capacity planning, Capacity forecasting, performance graphs and greater visibility into object relationships. Metric collection intervals should be granular and the platform should have capability to analyse metrics data captured at 5 min intervals or lesser over extended period of time, so that capacity planning and troubleshooting will be effective.	
10	The solution shall pre-emptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times	
11	The Solution should provide the health of the various relative subcomponents in a topology diagram which can be monitored and reported within the solution.	
12	The solution should provide alert management on problem detection. Each notification should include a clear description of the problem and provides remediation actions needed to restore service, degradations or failures are aggregated and correlated to workload/ virtual domains to enable a clear view of the impact of any issue.	
13	The solution should deliver a single interface for heterogeneous and highly scalable solution of both physical and virtual components with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting	
14	The solution should have the ability to provide information on aggregate and forecast capacity of the system both physical and virtual at any given time.	

15	The solution should provide capability of generating reports for usage, performance, compliance, health, forecasting, capacity, cost optimization across Private Cloud.	
16	The solution should provide capacity optimization capabilities to identify over-provisioned & under-provisioned resources and provide recommendations, alerts and automated actions on right-sizing and resource consumption so they can be right-sized for adequate performance and avoid resource wastage. Should provide visibility of capacity and VMs which can be reclaimed and cost visibility of the reclaimed capacity and VMs.	
17	The solution should provide out of the box capacity analytics and modelling, with granularity ranging from entire datacentre to cluster to individual host and virtual machine level.	
18	Single view of all virtual machines, allow Monitoring of system availability and performance and automated notifications with alerts. Monitor, analyse virtual machines, server utilization availability with detailed predict analysis of what's-if Scenario hardware procurement, capacity planning, Capacity forecasting, performance graphs and greater visibility into object relationships. Metric collection intervals should be granular and the platform should have capability to analyse metrics data captured at 5 min intervals or lesser over extended period of time, so that capacity planning and troubleshooting is effective	
19	The Solution should do analytics on capacity behaviour and should have capability of showing all under and over utilized VM's with their right sizing information on periodic basis.	
20	The Solution should be capable of creating custom dashboard with reporting as per customer ease and requirements, Solution should be able to scan/search objects with advanced search option for faster access to require information for trouble shooting	
21	Dashboards must be available to allow different Department to control the behaviour and consumption of the services	
22	The solution must allow single management console to view the performance of the infrastructure and the blueprint designer without logging in to different URL.	
23	The solution should provide resource reclamation functionality which identifies and reclaims inactive and abandoned resources by automating the decommissioning and reuse of retired resources. It should also provide reclamation savings reports which would enable organizations to quantify its cost savings	
24	The solution shall provide ready to use templates to validate configuration standards on the Virtual Machines covering security best practices, vendor hardening guidelines and regulatory mandates such as PCI-DSS, FISMA, CIS, DISA and custom compliance policies to track & enforce compliance.	

25	The solution should provide advanced trouble shooting capabilities leveraging AI/ML technologies which would provide troubleshooting evidence consisting of events, property changes and metric abnormalities. Should be able to trigger automated actions on event generation	
26	the Proposed Solution should be able to identified out of the box top 10 VM's basis on their high resource utilization (CPU/Mem/Storage/Network/IOPS) in a single dashboard	
27	The Solution have capability for finding object anomalies from standard behaviours and report this before major bottleneck for solution.	
28	Should have out of the box reporting features for current capacity usage, potential optimizations, physical resource availability, available headroom for expansion and system compliance to security/ operational guidelines.	
29	Should have capacity analytics which provide “What If" scenarios to identify the resource shortfall and do Capacity Planning for Future workload requirements.	
30	Should have ability to perform agentless services discovery for known services running inside OS and monitoring their states.	
31	The Solution should have Integrated log management and operation management, in order to better co-relate incidents happening and Should be able to perform Root Cause Analysis and corelation charts to detect deep issues with individual virtual machine, including Automated and Guided Remediations	
32	The Solution should be able to extend the monitoring and management capability to hardware environments such as 3rd party compute and storage, without any customization.	
33	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as Linux VMs, VM level encryption, secure boot, uninterrupted service delivery within and across datacentre at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology.	
34	Live Virtual Machine migration between different generations of CPUs in the same cluster with and without the need for shared storage option. Should support Live Virtual Machine migration long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.	
35	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another e.g.: FC, NFS, iSCSI, DAS.	
36	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	

37	Should support HA for migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software. Should support HA for VMs with a passthrough PCIe device or a NVIDIA vGPU.	
38	It should support affinity and anti-affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated.	
39	No downtime, no data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	
40	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.	
41	Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.	
42	Support for persistent memory, exposing it as block storage or as memory, to enhance performance for new as well as existing apps	
43	Should support features like DRS which run every minute and provides workload balancing.	
44	Should support network and storage QoS to ensure performance on per VM basis	
45	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and live vmotion.	
46	Should support TPM 2.0 and secure boot which provides protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.	
47	Should provide a trust authority which creates a hardware root of trust with a trusted computing base using a small, separately managed cluster of hosts. These hosts take over the task of attestation and will be the ones that verify the other clusters to ensure that those systems meet the requirements for trust.	
48	Should support Intel Software Guard Extensions (SGX) which allows applications to work with hardware to create a secure enclave such that things like encryption key cannot be viewed by the guest OS or hypervisor.	
49	Should support Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machines.	
50	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing, and disk array solutions.	

51	Should provide a centralized virtual switch which span across a virtual datacentre and multiple hosts should be able to connect to it. This should simplify and enhance virtual-machine networking in virtualized environments.	
52	In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
53	Should provide restful APIs which can be consumed with any automation tool like Puppet, Chef, Ansible.	
54	Provide Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 5 minutes.	
55	Solution should provide Kubernetes in the control plane of hypervisor for unified control of compute, network and storage resources to run both containers/native pods and virtual machines on the same platform	
56	It should provide unified visibility for VMs, Kubernetes clusters, containers from virtualization console for consistent view between Dev and Ops in virtualization platform. Centralized UI should support namespaces management with dedicated memory, CPU, and storage for each Application workload Kubernetes cluster.	
57	Solution should support for management, control plane and data plane integration with third-party partners in a wide variety of categories such as agentless antivirus, switching, operations and visibility, advanced security and more	

……

Signature of the authorized Signatory of Bidder

(Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 4B: APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED

(1.) Technical Specification of UTM (Next Generation FIREWALL):

S.NO	Specification	Compliance (Yes / No)
1	Next Generation Enterprise Firewall in HA	
2	The proposed vendor must have "Recommended" rating with min 97% Evasion proof capability and min 97% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Comparative Test Report. Proposed solution must be a Leader in the Gartner Magic Quadrant for the last 5 times.	
3	ICSA, FIPS, Common Criteria, FCC Class A, CE Class A, VCCI Class A, cTUVus and CB Certified	
4	The NGFW appliance should be of 1U or 2U rack space	
5	The offered firewall must be a single appliance and not a cluster and shall have dual power supply.	
6	The proposed NGFW solution architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware, CC#), Security processing (like apps, users, content/URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).	
7	The proposed firewall must have min 8 physical cores with x86 processor day 1. There should not be any proprietary ASIC based solution	
8	The device or any of its family should not have any feature of wireless within its hardware or software.	
9	The NGFW should have at least 120 GB solid-state drive for System storage	
10	Min 12 x 1G Copper interfaces from day 1, minimum 8 multigig ports 1G/10G SFP/SFP+ with 4 x 1Gig SFP SR transceiver, 4 x 10 Gig SFP+ SR transceiver from Day 1.	
11	Dedicated 1 x HA ports with direct attach cable of minimum 5-meter length in addition to requested data ports, OOB, Console Management and Micro USB/USB Port	
12	A Minimum NG Firewall application control throughput in real world/ production environment/ Application Mix – minimum 8 Gbps with 64KB HTTP transactions including Application-Identification/ AVC/ Application control and Logging enabled.	

13	Minimum NG Threat prevention throughput in real world/ production environment (by enabling and measured with Application-ID/ AVC, User-ID/ Agent-ID, NGIPS, Anti-Virus, Anti- Spyware, Anti Malware, File Blocking, Sandboxing, advanced DNS Security and logging security threat prevention features enabled – minimum 4 Gbps Throughput considering 64KB HTTP transaction size.	
14	IPsec VPN throughput – minimum 4 Gbps or more with 64KB HTTP transaction and logging enabled	
15	VLAN on single Gateway-4000	
16	New sessions per second – Min 100K considering 1-byte HTTP transaction size with AVC ON/ application override enabled or at least or minimum 600K Layer 3/ Layer 4 connections/ sessions per second	
17	Concurrent sessions – Min 900K which must be measured utilizing HTTP transactions or 5 Million Layer 3/ Layer 4 connection/ sessions	
18	The proposed solution will be a dedicated appliance to meet the required performance benchmark parameters i.e. throughput/ session count values. No clustering-based solution will be accepted by the department for achieving performance parameters	
19	Active/Active, Active/Passive and HA clustering support	
20	The proposed firewall shall support Dual Stack IPv4/ IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 - Should be able operate mix of multiple modes	
21	The proposed firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/ protocol/ evasive tactics.	
22	The proposed firewall shall be able to handle (alert, block or allow) unknown/ unidentified applications like unknown UDP & TCP. The proposed firewall should have the ability to create custom application signatures and categories directly on firewall without the need of any third-party tool or technical support. Also, the device should have capability to provide detailed information about dependent applications to securely enable an application	
23	The NGFW must have GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count	
24	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User id, Application id and threat protection profile under the same firewall rule or the policy configuration	
25	The firewall must support creation of policy based on wildcard addresses to match multiple objects for ease of deployment	

26	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application base on the content.	
27	The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.	
28	The firewall must disallow root access to firewall system all users (including super users) at all times.	
29	Solution should have machine learning capabilities on the dataplane to analyze web page content to determine if it contains malicious JavaScript or is being used for credential phishing. Inline ML should prevent web page threats from infiltrating network by providing real-time analysis capabilities.	
30	The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to inbound and inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood(Random Early Drop and SYN cookie), IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc	
31	All the proposed threat functions like IPS/ vulnerability protection, Antivirus, C&C protection etc should work in isolated air gapped environment without any need to connect with Internet.	
32	Should have protocol decoder-based analysis which can state fully decodes the protocol and then intelligently applies signatures to detect network and application exploits	
33	Intrusion prevention signatures should be built based on the vulnerability itself; A single signature should stop multiple exploits attempts on a known system or application vulnerability.	
34	Should block known network and application-layer vulnerability exploits	
35	The proposed firewall shall perform content-based signature matching beyond the traditional hash base signatures	
36	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every one hour	
37	All the protection signatures should be created by vendor base on their threat intelligence and should not use any 3rd party IPS or AV engines.	
38	Should be able to perform Anti-virus scans for HTTP, smtp, imap, pop3, ftp, SMB traffic with configurable AV action such as allow, deny, reset, alert etc	
39	Should have DNS sink holing for malicious DNS request from inside hosts to outside bad domains and should be able to integrate and query third party external threat intelligence data bases to block or sinkhole bad IP address, Domain and URLs	
40	Should support inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT)	

41	values and drop the packet based on Zone Protection profile	
42	The device should support zero-day prevention by submitting the executable files and getting the verdict back in five minutes post detection.	
43	The device should have protection for at least 20000 IPS signatures excluding custom signatures.	
44	Should have threat prevention capabilities to easily import IPS signatures from the most common definition languages Snort and Suricata	
45	The solution must be able to define AV scanning on per application basis such that certain applications may be excluded from AV scan while some applications to be always scanned	
46	The solution must have data loss prevention by defining the categories of sensitive information that is required to filter.	
47	Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data	
48	Vendor should automatically push dynamic block list with latest threat intelligence data base on malicious IPs, URLs and Domains to the firewall policy as an additional protection service	
49	The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following: · Automatically identify and block phishing sites · Prevent users from submitting credentials to phishing sites · Prevent the use of stolen credential	
50	The proposed Sandboxing solution can be an integrated firewall feature or the vendor can propose dedicated appliance to meet below requirement. There should be provision to enable the APT solution with following features. This could be a on premise or cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes. The cloud-based ATP solution should leverage only India based threat data lake.	
51	Advance unknown malware analysis engine should be capable of machine learning with static analysis and dynamic analysis engine with custom-built virtual hypervisor analysis environment	
52	Unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis	
53	The solution must be able to use AV and zero-day signatures based on payload and not just by hash values and it should support bare metal analysis if required using hybrid setup.	
54	The protection signatures created base unknown malware emulation should be payload or content base signatures that could block multiple unknown malware that use different hash but the same malicious payload.	

55	NGFW should protect against evasive techniques such as cloaking, fake CAPTCHAs, and HTML character encoding-based attacks	
56	NGFW should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use	
57	NGFW should support policy creation around end user attempts to view the cached results of web searches and internet archives	
58	NGFW should have a vast categorisation database where websites are classified based on site content, features, and safety in more than 70 benign and malicious content categories	
59	The architecture should ensure new protections and product updates are applied the instant they are released	
60	The Solution should have a consistent protection enforced by a single cloud engine for data in- motion and at-rest	
61	The solution should be natively integrated into existing control points; no need for ICAP, proxies, and additional infrastructure	
62	The Solution should have Out-of-the-box compliance templates like GDPR, CCPA, GLBA, financial regulations, etc.	
63	The solution should have extensive set of predefined industry-standard data identifiers and weighted regular expressions	
64	The solution should support machine learning-based data classification, automated deep learning, natural language processing, and AI models	
65	The solution should have capabilities of Exact data matching (EDM) and optical character recognition (OCR) for detection of structured and unstructured data	
66	Should support Multiple confidence levels and proximity analysis for high detection accuracy	
67	Flexible document properties for identification of third-party data classification tags	
68	Support for advanced Boolean operators for policy tuning	
69	The proposed firewall should have SSL decryption in Hardware and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	
70	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection	
71	The firewall must have the capability to be configured and deployed as SSL connection broker and port mirroring for SSL traffic	
72	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections	
73	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic	
74	The device should be capable of SSL automatic exclusions for pinned applications.	

75	The firewall supports TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection, Broker and SSL Decryption Port Mirroring.	
76	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well	
77	The proposed firewall must be able to operate in routing/NAT mode	
78	The proposed firewall must be able to support Network Address Translation (NAT)	
79	The proposed firewall must be able to support Port Address Translation (PAT)	
80	The proposed firewall shall support Dual Stack IPv4 / IPv6 (NAT64, NPTv6 or equivalent)	
81	Should support Dynamic IP reservation, tunable dynamic IP and port oversubscription	
82	L2, L3, Tap and Transparent mode	
83	Should support on firewall policy with User and Applications	
84	Should support SSL decryption on IPv6	
85	Should support SLAAC Stateless Address Auto configuration	
86	Should be IPv6 Logo or USGv6 certified	
87	The proposed firewall must support the following routing protocols: - Static - RIP v2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart	
88	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop and BGP peer address	
89	The firewall must support VXLAN Tunnel content inspection	
90	The firewall must support DDN provides such as DuckDNS, DynDNS, FreeDNS Afraid.org, Dynamic API, FreeDNS Afraid.org, and No-IP.	
91	The proposed firewall must have support for mobile protocols like GTP, SCTP and support for termination of GRE Tunnels	
92	The device should support load balancing of traffic on multiple WAN links based on application, latency, cost and type.	
93	The proposed solution must support Policy Based forwarding based on: - Zone - Source or Destination Address - Source or destination port - Application (not port based) - AD/LDAP user or User Group - Services or ports	

94	The proposed solution should support the ability to create QoS policy on a per rule basis: - by source address - by destination address - by application (such as Skype, Bittorrent, YouTube, azureus) - by static or dynamic application groups (such as Instant Messaging or P2P groups) - by port and services	
95	PIM-SM, PIM-SSM, IGMP v1, v2, and v3	
96	Bidirectional Forwarding Detection (BFD)	
97	The Solution should support DNS security in line mode and not proxy mode	
98	Solution should support database maintenance containing a list of known botnet command and control (C&C) addresses which should be updated dynamically	
99	DNS Security should support predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control	
100	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations	
101	It should support prevention against new malicious domains and enforce consistent protections for millions of emerging domains.	
102	The solution should support integration and correlation to provide effective prevention against New C2 domains, file download source domains, and domains in malicious email links. Integrate with URL Filtering to continuously crawl newfound or uncategorised sites for threat indicators. Should have OEM human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots. Should take inputs from at least 25 third-party sources of threat intelligence.	
103	Should support simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.	
104	Solution should support prevention against DNS tunnelling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection	
105	The solution should support capabilities to neutralise DNS tunnelling and it should automatically stop with the combination of policy on the next-generation firewall and blocking the parent domain for all customers.	
106	The solution should have support for dynamic response to find infected machines and respond immediately. There should be provision for administrator to automate the process of sink- holing malicious domains to cut off Command and control and quickly identify infected users.	

107	should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos	
108	The proposed firewall's SSL VPN shall support the following authentication protocols: - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML - Any combination of the above	
109	Should support on device and centralized management with complete feature parity on firewall administration	
110	There should be provision to permanently block the export of private keys for certificates that have been generated or imported to harden the security posture in order to prevents rogue administrators from misusing keys.	
111	The management solution must have the native capability to optimize the security rule base and offer steps to create application-based rules	
112	The proposed solution should support a single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.	
113	Data filtering, Content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities	
114	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis	
115	Should allow the report to be exported into another format such as PDF, HTML, CSV, XML etc.	
116	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs	
117	Should support creation of report based on SaaS application usage	
118	Should support creation of report based on user activity	
119	Should support creation of report based on custom query for any logging attributes	
120	OEM should be present in India from at least 5 years and should be proposed with 5 Years OEM support bundle with 24x7x365 days TAC support, RMA (There should be at least 4 RMA dept and one TAC for support in India), software	

	updates and subscription update support. The NGFW should be proposed with 5 years subscription licenses for NGFW, NGIPS, Anti-Virus, Anti Spyware, Threat Protection, APT Protection (Zero Day Protection with integrated Sandboxing), URL Filtering and DNS Security from day one. The solution shall support bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns for future use.	

(2.) Technical Specification of Server load balancer, WAF & GSLB:

S. NO	Item Description	Compliance (Yes / No)
1	The proposed solution shall be dedicated, Purpose built & hardware-based Solution with all components of the solution from same OEM only.	
1.1	High availability should be achieved using same make/ model license and same production licenses. There should not be use of any UAT/ test license on secondary device, all licenses should be production grade and active with all the functionalities. Proposed solution should work in Active-Active mode. All components of the proposed solution should be from same and single OEM only.	
2	Should be high performance multi-tenant hardware with multicore CPU support. Platform should support multiple network functions including application load balancing, global server load balancing, SSL VPN, Zero Trust Access and Web application Firewall. Appliance should be purpose-built hardware to support desire functionality of Server load balancing and WAF using Kubernetes based multi tenancy platform.	
3	The appliance should have minimum 2*40G/100G QSFP+ & 8*10G/25G SFP+	
4	Appliance should support L7 requests per second: 2.5M on day 1 scalable to 4.3M with license upgrade on same hardware device	
5	Appliance should support L4 connections per second: 1M on day 1 scalable to 1.8 M with license upgrade on same hardware device	
6	Appliance should support L4 HTTP requests per second: 15M	
7	Appliance should support Maximum L4 concurrent connections: 72M on day 1 scalable to 100 M with license upgrade on same hardware device	
8	Appliance should support Throughput: 95 Gbps/60 Gbps L4/L7	

9	Appliance should support 35 Gbps bulk SSL encryption and 35 Gbps compression on Day 1 scalable to 50 Gbps bulk SSL encryption and 50 Gbps compression with license upgrade on same hardware device	
10	Appliance should support ECC†: 30K TPS (ECDSA P-256) / RSA: 60 K TPS (2K keys) scalable with license upgrade on same hardware device to ECC†: 70K TPS (ECDSA P-256) / RSA: 100 K TPS (2K keys)	
11	Appliance should support Virtualization upto 8 instances scalable to 26 instances with license upgrade	
12	Appliance should have integrated redundant hot swappable power supply.	
13	The product should comply and support Dual Stack IPv4 and IPv6 both	
14	The solution should have support for multiple VLANs with tagging capability	
15	The device should have support for bonding links to prevent network interfaces from becoming a single point of failure (e.g LACP)	
Server Load Balancing features & GSLB		
16	Solution should support various deployed mode like one- arm mode, routed mode or DSR mode	
17	Should able to load balance both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.	
18	The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SIP session ID, hash header etc.	
19	The proposed solution must support global server load balancing between DC and on-premise/ cloud-based DR and should support following DNS Record type - All (A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV, TXR)	
20	5 Year OEM Support (24X7)	

(3.) Technical Specification of Internal Firewall

S No.	Item Description	Compliance (Yes / No)
General Requirement		
1	The solution be reported as LEADER in the leading Industry benchmarking report for any one year in the last five published reports.	

2	The Firewall appliance should have certifications like NDPP or EAL4 or more.	
3	Proposed solution should not declare with eol, eos or end of support by OEM.	
Technical Specification		
4	Stateful inspection firewall throughput (multiprotocol) should be min 20 Gbps.	
5	The firewall should provide 8 Gbps of Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection and logging enabled on IMIX / Enterprise Mix / Production Traffic with all License enabled.	
6	Firewall Should have SSL Inspection (HTTPs Inspection of at least IPS module) throughput of minimum of 7Gbps mentioned in public Datasheet.	
7	The solution shall provide up to 10 Gbps of IPS throughput with Enterprise Mix traffic.	
8	Firewall Solution should have VPN throughput of at least 50 Gbps.	
9	Firewall shall support up to 7 million Concurrent connections.	
10	Should be able to support 450,000 connections per second.	
11	Firewall License proposed must include all required features given in tender.	
12	Should have 8x 1GE RJ-45 interfaces, 4x 10GE SFP+ populated with SR, 1xGE Management & 1 Console interfaces with auto sensing capacity and option to expand further.	
13	Should have at least one Management and console port.	
14	Should have at least 1024 supported VLAN.	
Firewall Features		
11	Should have Layer 3 and Layer 4 stateful firewall inspection including access-control and network address translation and port address translation.	
12	Should have Multiple Security zones, security policies, port scan filtering.	
13	The solution should have network attack detection also provide Protection against IP Attacks: IP, ICMP, TCP protection.	
14	Provide protection against: - Denial of service (DoS) and Distributed denial of service (DDoS) protection - ICMP, UDP, SYN/TCP, SYN Cookies Protection. - IP spoofing protection.	
15	The product should have Content Filtering Based on MIME type, file extension, and protocol also Transparent Mode support.	

16	Support protocols like Static routes. - RIPv2 +v1 , RIPng, OSPF/ OSPFv3, BGP, Multicast (Internet Group Management Protocol IGMPv1/2/3), PIMSM/ DM/ SSM, Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP), source-specific, Multicast inside IPsec tunnel, MSDP. - MPLS (RSVP, LDP, Circuit Cross-connect (CCC), Translational Cross-connect (TCC), Layer 2 VPN (VPLS), Layer 3 VPN, VPLS, NGMVPN).	
17	Product should support Address Translation: - Static NAT, Source and Destination NAT with Port Address Translation (PAT). - Persistent NAT, NAT64.	
18	Support IPv6	
19	Must support NAT (SNAT and DNAT) with following modes: Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat & 64 (IPv6- to-IPv4)	
20	The Proposed firewall Solution should be able to work in High Availability (HA) mode & operate on either Transparent (bridge) mode or NAT/Route mode.	
21	Appliance should support an LCD panel/ LED to display alerts and fault information for an administrator to monitor the system.	
22	The appliance should have redundant power supply.	
23	The Device management should support SSH, HTTPS SNMP v1/ v2c/ v3 Standard CLI and Secure Web GUI Interface TACACS+ and RADIUS authentication Syslog Support.	
License and Support		
24	The Proposed device Solution should be provided with hardware replacement warranty and Ongoing Software Upgrades for all major and minor releases during the completion of project	
25	The IPS detection methodologies shall consist of: - Signature based detection using real time updated database - Anomaly based detection that is based on thresholds - Support One-arm IDS (sniffer mode)	
26	Configurable IPS filters to selectively implement signatures based on severity, target (client/ server), protocol, OS and Application types.	
27	The proposed system should be able to block, allow or monitor only using IPS, Application Control or AV scanning and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:	

28	AV Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available.	
29	The Propose Antivirus protection shall include advance malware protection: - Virus Outbreak Protection - Content disarm and reconstruction (CDR)	
30	The proposed system shall have the ability to detect, log and take action against network traffic based on over 2,000 application signatures	
31	The application signatures shall be manual or automatically updated	
32	The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/ or logged when passing through the unit. The DLP capability shall support the following protocol & activities: - HTTP/ HTTPS POST, HTTP/ HTTPS GET - FTP PUT, GET - SMTP, IMAP, POP3, SMTPS, IMAPS, POP3S	
33	Solution should support build in next generation security features like Firewall, IPS, Web/ URL filtering, SSL decryption, antivirus, antimalware, DNS filtering, Application control from day 1.	
34	The system shall support two factor authentications for admin users and should provide two 2FA tokens from day 1	
35	Proposed firewall should have SD WAN functionality from day one and should allow the use the most preferred link based upon Link characteristics (Latency, Jitter, Packet loss) for critical applications as defined in policy. Any license needed to have SD WAN features should be consider from day one	
36	The proposed OEM firewall solution should have capability to integrate with firewall analyzer tools like Tufin, Algosec etc. whenever required in future without any cost implications. Bidder need to provide publicly available website link or document as a proof.	
37	The proposed product or product family or operating system should be FIPS 140-2 or higher certified.	
38	OEM should have Local Stocking of Spares within the Country to ensure that the SLA is not breached	
39	OEM of the Proposed Solution Vendor should provide	

	regular updates to geolocation database from their public downloads website	
40	OEM should have a Technical Assistance Center (TAC) which Follow the Sun Model with toll free numbers	
41	The Support should be of production/Enterprise support level. For Highest Priority Calls (P1 Calls), response to be provided by OEM/ Bidder within 15 minutes. The Expected resolution Time is 4 hours (maximum).	
42	OEM should have Support Centers / Service Center in India	
43	The devices and software support should be provided for 5 years after deployment.	

(4.) Technical Specification of L3 Switching

S.NO	Details	Complied (Yes/NO)
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2	Switch should support the complete STACK of IPv4 and IPv6 services.	
3	The Switch used have the capability to function in line rate for all ports	
4	Minimum 48 ports support 1/10/25 Gbps SFP/SFP+/SFP28 ports for host connectivity and 6* 40/100G ports for Fabric/Spine connectivity. The proposed switch should support native 25G and should be populated with 48*25G Multimode fiber trans receivers for downlink connectivity & minimum 2*100G ports with multimode 100G Transceivers, for uplink connectivity.	
5	Switch should have console port for local management & management interface for Out of band management	
6	1 RU fixed form factor	
7	Switch should be rack mountable and support side rails if required	
8	Switch should be provided with power redundancy	
9	Modular OS with dedicated process for each routing protocol	
10	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	
11	Switch should support minimum 1000 VRF instances with route leaking functionality	
12	The switch should support 400k IPv4 LPM routes	
13	The Switch should support intelligent buffer management with a minimum buffer of 40MB.	
14	The switch should have MAC Address table size of 90k	
15	The switch should support 8K multicast routes	

16	Switch should support 64 nos of ECMP paths	
17	Switch should support minimum 1 Tbps of switching capacity (or as per specifications of the switch if quantity of switches is more, but should be non-blocking capacity)	
18	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN	
19	Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre	
20	Switch should support Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) and VLAN Trunking (802.1q)	
21	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
22	Switch should support minimum 90k of MAC addresses	
23	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
24	Switch should support layer 2 extension over VXLAN across all DataCenter to enable VM mobility & availability	
25	The Switch should support DC Briding i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
26	The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
27	Switch should support static and dynamic routing	
28	Switch should support segment routing and VRF route leaking functionality from day 1	
29	Switch should support Segment Routing and Layer3 VPN over Segment Routing	
30	Switch should support multi-instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
31	Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM	
32	Support Multicast Source Discovery Protocol (MSDP)	
33	IGMP v1, v2 and v3	
34	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)	

35	Switch should support for different type of QoS features for real time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
36	Switch should support Rate Limiting - Policing and/or Shaping	
37	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
38	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
39	Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
40	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
41	Switch platform should support MAC Sec (802.1AE) encryption in hardware	
42	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
43	Switch should support IP Source Guard to prevents a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	
44	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
45	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
46	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
47	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
48	Should support Should support software telemetry that is not SNMP based and telemetry should be provided without impacting performance of the switch and without adding overload on the resources like CPU and Memory.	

49	Switch should provide below telemetry features: •Full Inventory like Global, fabric, switch, ports, endpoints, VMs, L3 neighbors, IPv4/v6 routing table etc. •Verified Scale limits with Hardware/software lifecycle & EoS. •Network Topology and Utilization of Operational like MAC/Route & Hardware resources like port utilization/ BW •Switch Anomolies related with Advisories , PSIRT and Field Notices •Software upgrade check with TAC assist •Latency and flow •Bug Scanning , Switch's CAM Analyzer, Microbursts and log collector •Real Time Interface statistics like CPU, memory, power, temperature, and interfaces with historical information. •Switch and fabric-level power consumption, cost (kWh), and CO2 emissions CO2 emissions.	
50	All the components should be from same OEM for ease of management and interoperability	

(5.) Technical Specification of Top of the Rack switch

S.No	Item Description	Compliance (Yes/No)
1	TOR Switch Specification (2 Qty) Ports per TOR switch shall be configured with required licenses and compatible cables as below: •Minimum 48 port Switch with 24 x 10G Short Range SFP+ populated •Minimum 2 x 10Gb / 40 G or higher QSFP+ with required no of DAC's minimum 3m in length per switch for Core to TOR and Core to Core interlink •12 no's of cables minimum 5m in length per switch for connectivity of TOR switches. •Bidder needs to ensure sufficient ports are available for uplink to Core Switch •The TOR Switches must be Data Center grade switches with all required features to support virtualized compute environment.	
2	TOR Switch Features • Proposed Switches should be Data Center Class Switches and not Campus Switches •Should support IPV6 routing protocols	

	•Should support Jumbo frames on all ports •Each Switch must be provisioned with adequate hot swappable power supplies and cooling in redundant mode for the optimal system performance.	
3	High Availability: Should support Active-Active, Active-Passive, Clustering, Stacking	
4	Should be compatible with Proposed Solution & meets all the requirements	
5	Rack Mountable. 1 or 2 RU	
6	Operating Temperature Range (Degree C) 45	
7	Operating Humidity (RH) (%) e 85	
8	On Site OEM Warranty (Year) 5	
9	End of Life and End of support Should not be next 5 years.	

(6.) Technical Bid for Server Security:

S.No	Technical Specifications	Compliance Yes/No
1	Proposed server security solution should be on-premise with capabilities of Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention and recommendation scan. All functionality must be available in single agent	
2	The proposed server security solution must support broad range of OS platforms of server operating systems i.e. Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Solaris, AIX, Amazon Linux etc.	
3	The Proposed solution should support various OS versions - Microsoft Windows Server (2008 & 2008 R2, 2012 & 2012 R2, 2016, 2019, 2022), Red Hat Enterprise Linux (6,7,8,9), Solaris (10.0,11.0,11.1,11.2,11.3,11.4), Oracle Linux (6,7,8,9), AIX (6.1,7.1,7.2, 7.3), CentOS (6,7,8) and Suse Linux (12,15), Redhat OpenShift (4.9-4.13), Rock Linux (8-9), Debian Linux (8-12), Cloud Linux (7,8), Amazon Linux 2 (Graviton 2/3, 2023), AlmaLinux (8,9).	
4	The firewall shall be bidirectional for controlling both inbound and outbound traffic and should have the capability to define different rules to different network interfaces	
5	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans and should support stateful inspection functionality	
6	Solution should provide policy inheritance exception capabilities and ability to lock computer (prevent all communication) except with management server.	
7	Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.	
8	The firewall should be able to detect protocol violations of standard protocols and provision inclusion of packet data on event trigger for forensic purposes.	

9	Solution should have security profiles that allows firewall rules to be configured for groups of systems, or individual systems.	
10	The proposed solution should support Deep Packet Inspection (HIPS/IDS) and should support creation of customized DPI rules if required.	
11	Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.	
12	Virtual Patching should be achieved by using a high- performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.	
13	Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.	
14	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (Eg. Selecting rules, configuring policies, updating policies, etc.)	
15	Solution should provide recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	
16	The solution should allow imposing HTTP Header length restrictions and have the capability to inspect and block attacks that happen over SSL.	
17	The solution should allow or block resources that are allowed to be transmitted over http or https connections and capable of blocking and detecting of IPv6 attacks.	
18	Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.	
19	Solution should offer protection for virtual, physical, cloud & docker environments.	
20	Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).	
21	Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.	
22	Solution should work in Tap/detect only mode and prevent mode and support automatic and manual tagging of events also have CVE cross referencing when applicable for vulnerabilities.	

23	Solution should provision inclusion of packet data on event trigger for forensic purposes and shall protect against fragmented attacks also should allow to block based on thresholds	
24	Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.	
25	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/ Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto- Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.	
26	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions.	
27	The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.	
28	Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).	
29	Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.	
30	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	
31	Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required.	
32	Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.	
33	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.	
34	Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture.	
35	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.	
36	Solution should support the following: Multiple groups of hosts with identical parameters, Regex or similar rules to define what to monitor, Ability to apply	

	a host template based on a regex of the hostname, Ability to exclude some monitoring parameters if they are not required, Ability to generate E Mail and SNMP alerts in case of any changes, Solution should support creation of custom Integrity monitoring rule and Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.	
37	Anti-malware should support Real Time, Manual and Schedule scan and should have flexibility to configure different real time and schedule scan times for different servers and should have feature to try & backup ransomware encrypted files and restoring the same as well.	
38	Solution should support excluding certain file, directories, file extensions from scanning (real time/schedule) and use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.	
39	Solution should support True File Type Detection; File extension checking and have heuristic technology blocking files containing real-time compressed executable code.	
40	The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning	
41	The proposed solution should be able to perform behavior analysis for advanced threat prevention and have its own threat intelligence portal for further investigation, understanding and remediation an attack.	
42	Solution deployment should cause limited interruption to the current network environment also should have Ransomware Protection in Behavior Monitoring.	
43	Solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.	
44	Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events.	
45	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.	
46	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/ un-assignment of rules when not required.	
47	Solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/ Windows servers use the same base security profile allowing further fine tuning if required.	
48	Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.	
49	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.	
50	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.	

51	Ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.	
52	Solution must support decoders for parsing the log files being monitored.	
53	Solution should allow administrators to control what has changed on the server compared to initial state and should prevent unknown and uncategorized applications from running on critical servers also must support Global Blocking on the basis of Hashes and create blacklist for the environment.	
54	Solution should have option to allow to install new software or update by setting up maintenance mode and should have ability to scan for an inventory of installed software & create an initial local ruleset.	
55	Change or new software should be identified based on File name, path, time stamp, permission, file contents etc. and must have ability to enable maintenance mode during updates or upgrades for predefined time period.	
56	Logging of all software changes except when the module is in maintenance mode and Should support Windows & Linux operating systems.	
57	Should have the ability to enforce either Block or Allow unrecognized software and must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.	
58	solution must be able to block all communication to Command & control center and must be able to identify communication over HTTP/ HTTPS protocols and commonly used Http ports.	
59	Solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and Solution must have an option of assessment mode only so that URLs are not blocked but logged.	
60	solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's.	
61	The solution shall be able to deliver all the above-mentioned features like Anti- malware, Host Based Firewall/ IPS, File Integrity Monitoring, Log Inspection & Application control in a single agent.	
62	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.	
63	Any policy updates pushed to the agent should not require to stop the agent, or to restart the system and Solution should provide ability to hide agent icon from getting displayed in system tray.	
64	The solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.	
65	The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organization's data center environment.	
66	The proposed solution should be managed from a single centralized web-based management console.	

67	The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.	
68	The solution shall allow to do all configurations from the central management console including, but not limited to enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.	
69	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.	
70	Should support integration with Microsoft Active directory and should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.	
71	Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL.	
72	The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.	
73	The solution should support forwarding of alerts through SNMP, E-Mail and should be able to generate detailed and summary reports.	
74	The solution shall allow scheduling and E Mail delivery of reports and should have a customizable dashboard that allows different users to view based on their requirement.	
75	The solution should support Web Services if it is required to export data out to other custom reporting solutions and shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.	
76	Administrators should be able to selectively rollback rules applied to agents and should maintain full audit trail of administrator's activity.	
77	Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.	
78	The solution shall allow updates to happen over internet or shall allow updates to be manually imported in the central management system and then distributed to the managed agents. Additionally, solution must also have an option of defining machine to be updater relay only.	
79	Proposed solution should also provide SAAS based container security solution.	
80	Container security should provide protection for containers at all stages of their lifecycle, during deployment, at deployment, after deployment and at runtime.	
81	Container images should be scanned as part of development pipeline and to perform ongoing scans of images in your registries so that developers can detect and fix security issues early in the container image lifecycle	
82	Container image scanning should check vulnerabilities, malware, compliance violations, secrets and keys.	
83	Container Security should provide policy-based deployment control to ensure the Kubernetes deployments run in your production environment are safe.	

84	When an image is ready to be deployed with Kubernetes, the admission control webhook should be triggered checking whether the image is safe to deploy and either allow or block it from running.	
85	Container Security should check the policy assigned to the cluster on a regular basis, ensuring that running containers continue to conform to the defined policy. If there are changes to the policy after the initial deployment, the updated policy should be enforced. Running containers are also checked for new vulnerabilities as they are discovered.	
86	Container runtime security should have a set of pre-defined rules that provide visibility into MITRE ATT&CK® framework tactics for containers, as well as container drift detection.	
87	Proposed Container security should provide visibility of operating system and open source code vulnerabilities that are part of containers running in clusters where Container Security is installed.	
88	The Proposed Server security solution should be Leader in server security market as per IDC latest report	
89	The Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per latest Frost & Sullivan Reports	
90	The proposed OEM should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years	
91	OEM must have contributed at least 50 zero day/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publicly available.	
92	The proposed Server security solution should be EAL 2 + certified	

(7.) Technical Specification for DAM:

S N	Specifications	Compliance (Y/N)
1	DAM solution should treat if one database having one or more different instances as single database. Also, number of cores will not be counted for a particular database rather the same should be considered as single database.	
2	The solution should meet regulatory compliance such as RBI guidelines on cyber security, PCI DSS, Data Privacy Law, GDPR, Industry best practices etc.	
3	Creation of an inventory through auto discovery of all Oracle, MSSQL, MySQL databases and database users, deployed across the enterprise.	
4	The proposed DAM solution should be able to monitor in scope structured database without dropping any log.	
5	Proactive discovery and classification of sensitive information across databases and prevent access to sensitive data as per company's policy	
6	The architecture should adopt scale-out approach to accommodate additional databases in future.	

7	The DAM solution should be able to process minimum 10,000 TPS (transactions per second) and must support any increase in transactions during the complete contract period. Additionally, intermediate levels of solution should monitor privileged and non-privileged	
8	The solution should be able to factor/scale additional licenses in the event that the TPS rises (for the same number of DBs Servers). This should be carried out without any additional cost to the company.	
9	The solution should have the capability to detect vulnerabilities and identify issues such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Further, comprehensive reports should be provided along with suggestions to address all vulnerabilities.	
10	The solution should provide capability to detect DB attacks and prevent attacks such as SQL injection, leakage of sensitive data etc. and also should be able to detect and alert unauthorized or unusual queries, access to sensitive and confidential data etc. for various databases including big database.	
11	The solution should have centralized management of database agents to monitor the health throughout the life cycle of the agents	
12	The solution should support installation manager on each database server to avoid manual efforts to coordinate agent activities along with up-gradation and configuration changes.	
13	The solution should be able to monitor and detect breaches/ anomalies for all the structured databases like MSSQL, MySQL, Oracle DB etc.	
14	The solution should identify, auto-classify the data/ database-objects based on confidentiality, sensitivity of data based on PII, ISO 27001, data privacy or custom parameters.	
15	The solution should be capable of performing real-time monitoring and recording of all privileged activity like DDL, DML and DCL, Schema Creation, modification of accounts/ roles and privileges.	
16	The solution should capture and analyse all database activity, from both application user and privileged user accounts, providing detailed audit trails that shows the “Who, What, When, Where, and How” of each transaction.	
17	The solution should have policy enforcement while executing SQL statements and should give flexibility to whether to allow, log, alert or block the SQL.	
18	The solution should allow grouping of the database objects and accordingly allow implementing various rules.	

19	The solution should be able to manage & control Database access by IP, user, time, date etc. and should be capable of traffic filtering, categorization of traffic based on custom parameters like data interface, NIC, ports, source users, source IP etc.	
20	Minimum usage of system resources: For agent-based system, CPU utilization on the DB server should not exceed 5% beyond present utilization, however, the same should be configurable. For network monitoring the impact on monitored servers should be zero. At the same time, the solution should not overload the network and delay real time monitoring and attack mitigation measures. The solution should provide capping capabilities for CPU, RAM and disk on the agent-based solution.	
21	The solution should be able to integrate with leading NGSOC solutions such as SIEM etc. to generate meaningful correlated events. Also, it should be able to integrate with PIM.	
22	The solution should be able to integrate with external ticketing management tools for managing change.	
23	The solution should be centrally manageable from a single console including update of agents, pushing upgrades, patch updates, configurations updates, policy updates, start/ stop/ restart etc.	
24	The solution should have capability to build an inventory by discovery of all the databases and database users. The discovery supported by it should be both auto discovery and on demand discovery.	
25	The solution should have the ability to generate report consisting of the details of all the databases like IP address, Database type, Agent version, status (active/inactive) and timestamp of last communication.	
26	The solution should detect sensitive data types as defined by the company such as user ID, email address, passwords, etc., in database objects	
27	The solution should enable segregation of duty in terms of account management, security administration and database administration.	
28	The solution should have various notification mechanisms like SMS, Mails, SNMP traps, long IP block etc. for security monitoring and health monitoring and the notification mechanism must be real time.	
29	The 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.	
30	The solution should have the ability to generate report showing the access of each user to the tables of each database along with the user who granted them the permission.	

31	The solution should store all audit logs in tamper-proof flat file format and have faster retrieving process for reporting purpose.	
32	The proposed solution should support both monitoring and blocking mode within same agent and without having any other component.	
33	Solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes	
34	DAM solution should identify abnormal server and user behaviour and providing early detection of possible attacks using outliers. For example: (a) User accessing a table for the first time User selecting specific data in a table that he has never selected before (b) Exceptional volume of errors (c) Activity that itself is not unusual, but its volume is unusual (d) Activity that itself is not unusual, but the time of activity is unusual	
35	Solution must support filtering/hiding of the bind variables of all the SQL activities captured	
36	The solution should not store sensitive data in plain text in logs generated by the application (e.g. passwords) Logs and audit-trail generated by the solution should not be editable by users/ administrator and should be read-only.	
37	The Proposed Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.	
38	Solution must be able to monitor database which run on non-standard port.	
39	The solution should be able to auto discover default passwords in the default DB accounts	
40	Solution track the dormant accounts as per defined rule.	
41	The solution should inspect both in-coming and out-going DB traffic, compare with the rules and generate alert.	
42	Solution should detect attacks on network protocols, as well as application layer DB activity.	
43	The solution should provide full details needed for analysis of audited events: date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. should be capable of capturing and reporting at a very granular level.	

44	Solution should detect attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to issue an alert and\ or terminate the session in real time	
45	The solution should discover misconfigurations in the database and its platform and suggest remedial measures.	
46	Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.	
47	Solution should also be able to detect any change happens in stored procedure	
48	Solution should have capability to monitor local access & encrypted connections (Oracle ASO, SSL, IPSec etc.)	
49	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.	
50	Ability to mask or obfuscate Sensitive data in the result sets to the user.	
51	The solution should support creation of different type of security and audit policies such as rule report based on heuristic and content based. These policies should support customization.	
52	The proposed solution should support Monitoring Mode and blocking Mode of Deployment. In monitoring mode, solution can generate alerts for unauthorized activity. In blocking mode, solution must proactively block the queries including blocking of matching signatures for known attacks like SQL injection.	
53	There should be no down-time of the OS or database for deployment of agents.	
54	The agent should not require a reboot of OS and DB after installation / configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. The solution should not use any 3rd Party software/ support for any purpose	
55	If the communication between agent and the console is lost, immediate alert to be issued.	
56	The solution should not use the native database audit functionality. The Solution should not employ native database transaction log auditing.	

57	The solution should be able to support/monitor all database activities in OS like AIX, UNIX, Linux, Solaris, Windows and Databases like Oracle, MS- SQL, MySQL, PostgreSQL at a minimum provided that DB vendors still support the versions in scope	
58	The solution should provide information of DB links and should have capability to monitor the activity of DB links	
59	The solution should generate alert for any violation of security policy real time	
60	All the reports should be generated at least in minimum time (within 120 seconds)	
61	The solution should discover all the databases with details i.e. IP, type, OS, available in the company network	
62	The solution should also discover if any new database and DB objects created within the monitored network/systems.	
63	The solution must allow administrators to add and modify policies.	
64	The solution should log the actual client IP.	
65	The solution support individual user access auditing for packaged applications like SAP, Peoplesoft etc.	
66	Separate policies should be applied for different databases configured in DAM	
67	The solution should have pre-built templates for well-known security and audit policies.	
68	The Solution should integrate existing 8 databases & include future requirement (if any). Solution should support the deployment modes i.e. monitoring / blocking separately for each database	
69	The solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc.	
70	Rules also should allow blocking access depending upon different parameters like above.	
71	The Proposed Solution should include a browser based single administration interface.	
72	The Proposed solution should have an out-of-band management capability, in case of appliance for the solution	
73	The Proposed Solution should be managed centrally within DR Setup.	
74	Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties. i.e. Administrator (Super- User), Manager, read only etc.	
75	The solution should support the following authentication mechanism for accessing the solution:	

	(i) In-built authentication in the solution	
	(ii) Kerberos authentication	
	(iii) LDAP/AD authentication	
	(iv) RADIUS authentication	
76	The company should be able to deploy or remove the DAM solution from the network with no impact on the existing databases or the network architecture.	
77	Support proper reporting and logging facilities.	
78	Should be able to report events and alerts via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.	
79	The solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible. For example, the Username placeholder looks like (${Alert.username})	
80	The solution must support generation of both predefined as well as customize reports as per customer requirements in PDF & CSV format.	
81	Alert should be generated in case of violation of rules through SMTP (mail).	
82	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.	
83	Solution must support either: 1) Ability to query raw event data via REST API, 2) Ability to perform bulk exports of raw event data, or 3) Other external analytical and data store integration method.	
84	Solution should provide monitoring of all on-prem supported databases.	
85	Solution should provide good compression ratio to store logs which will require minimum infra and should have ability store the log online for multiyear retention requirement	
86	Solution should not write any logs on the database server when using agent-based monitoring	
87	The solution should have a lean architecture with minimal moving parts, supports structured data flexible to support both Agent based and Agentless environments	

88	The solution should automate and simplify regulatory compliance activities and provides superior long-term retention of live audit data in the DAM. It should enable long-term data estate and forensic records retention policies (e.g., fast access, live audit data, length of retention timeframes).	
89	The solution should establish critical database security visibility and should only send events to SIEM rather than the entire logs. The solution should reduce SIEM index/telemetry fees with compute and storage costs.	
90	Advanced Features	
91	Ability to kill sessions for accessing sensitive data/ policy violations and keeping all activity in the logs	
92	Communication from Agent to management server must be encrypted.	
93	If the agent mal-functions or uninstalled or disabled on server, immediate alert to be issued.	
94	Sensitive Data Management	
95	The solution should be capable of auto discovering sensitive/ confidential data like Aadhaar or any PII in the database and offers the ability for customization.	
96	The solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts.	

(8.) Technical Specification for DR Replication Software:

S.NO	Details	Complied (Yes/NO)
1	Continuous data protection with near-zero recovery point objectives (RPO).	
2	Automated failover and failback procedures.	
3	Real-time replication to ensure data consistency and availability.	
4	Solution should integrate directly with the hypervisor (e.g., VMware), eliminating the need for additional agents or appliances.	
5	Support for various virtual environments (VMware vSphere, Microsoft Hyper-V).	
6	Integration with existing infrastructure including storage systems and network configurations.	
7	Should have capabilities of replicating a single VM to multiple target platforms simultaneously.	

8	Ability to scale to accommodate future growth in data volumes and infrastructure changes.	
9	Granular recovery options allowing restoration at different levels (files, applications, entire VMs).	
10	Point-in-time recovery to enable rollback to specific instances before data corruption or loss.	
11	Minimal impact on production environment during replication and recovery operations.	
12	Encrypted data transmission to ensure security during replication.	
13	Role-based access control for secure management.	
14	Operational Requirements	
15	Centralized management console for monitoring and controlling replication tasks.	
16	Automated alerting and reporting features.	
17	Support and Maintenance	
18	5Years of 24/7 technical support from the vendor.	
19	Regular software updates and patches.	

Annexure – 5: Price / Financial Bid Format for DR SETUP

APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED

(Must be submitted in the 3rd sealed envelope)

ENTITY NAME: _____

ADDRESS: _____

CONTACT PERSON: _____ PHONE NUMBER: _____

EMAIL: _____ WEB SITE: _____

We submit our Price/Financial bid (fees) for the proposed assignment as under for

(I). DR Environment

Components	Part No	Descriptions	Quantity	Unit Price	Total
Servers					
Storage					
Virtualization Software			14		
UTM/ IPS/IDS			1		
WAF + GSLB + SLB			1		
Internal Firewall			1		
Layer 3 Switch			1		
Layer 2 Switch			1		
Server Security		(Quantity as per solution requirement)			
DAM		(Quantity as per solution requirement)	1		

Add any other line item with description and supporting documentation/ Annexure required for your solution and migrating existing services					
	Grand Total				

** The quantities may be modified as per solution requirement proposed.

(II). DR - Data Centre hosting services:

S.No	Descriptions	Months	Per Month Cost	Total
1	Hosting charges for the datacenter with required quantity of racks (Bidder shall attach detailed Bill of Material as line item with cost)	60		
2	Electricity on Actual			
			Grand Total	

** SI shall provision and submit comprehensive hardware, licensing and other solution requirements for above.

……

Signature of the authorized Signatory of Bidder

(Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 6 : Proforma Bank Guarantee For Performance

(On Non-Judicial stamp paper of value Rs.500/-)

Bank Guarantee No.:---------- Dated: ----------

To, ECGC Limited

CTS No. 393, 393/1-45,

Village Gundavali, M.V. Road,

Andheri (East), Mumbai – 400069

Reference: - Contract No.----------, awarded on ----------

IN CONSIDERATION OF ECGC LIMITED, a company incorporated under the Companies Act 1956 and having its registered office at ECGC Bhawan, CTS No. 393, 393/1-45, M.V. Road, Andheri (East), Mumbai, PIN 400069, Maharashtra, India. (hereinafter referred to as the "the Company" which expression shall, unless it be repugnant or contrary to the subject or context thereof, be deemed to mean and include its successors and assigns) having selected Messers..... a partnership firm / a company registered under the Companies Act, 1956/2013 having its Registered office at ..... (hereinafter called the Vendor which expression shall, unless it be repugnant or contrary to the subject or context thereof, be deemed to mean and include its successors and assigns) vide Agreement dated _____ (hereinafter called as "the Work Order" which expression shall include any amendments/alterations to "the Work Order" issued by "the Company") for the work as stated in the Scope of Work in Request for Proposal (hereinafter called as RFP)**FOR APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED** as stated in the said Work Order and the Purchaser having agreed that the Vendor shall furnish a security for the performance of the Vendor's obligations and/or discharge of the Vendor's liability in connection with the said Work order and the Company having agreed with the Vendor to accept a performance guarantee,

1. We, ... Bank having office at ..... (Hereinafter referred to as "the Bank" which expression shall include its successors and assigns) hereby agree to pay to the Company without any demur on first demand an amount not exceeding Rs..... Rupees .....

only) being 100% of the order value against any loss or damage, costs, charges and expenses caused to or suffered by the Company by reason of non-performance and non-fulfilment or for any breach on the part of the Vendor of any of the terms and conditions of the said order.

2. We, ... Bank further agree that the Company shall be sole judge whether the said Vendor has failed to perform or fulfil the said order in terms thereof or committed breach of any terms and conditions of the order and the extent of loss, damage, cost, charges and expenses suffered or incurred or would be suffered or incurred by the Company on account thereof and we waive in the favour of the Company all the rights and defenses to which we as guarantors may be entitled to.

3. We, ... Bank further agree that the amount demanded by the Company as such shall be final and binding on the Bank as to the Bank's liability to pay and the amount demanded and the Bank undertake to pay the Company the amount so demanded on first demand and without any demur notwithstanding any dispute raised by the Vendor or any suit or other legal proceedings including arbitration pending before any court, tribunal or arbitrator relating thereto, our liability under this guarantee being absolute and unconditional.
4. We, ... Bank further agree with the Company that the Company shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said order/or to extend time of performance by the Vendor from time to time or to postpone for any time to time any of the powers exercisable by the Company against the Vendor and to forbear to enforce any of the terms and conditions relating to the order and we shall not be relieved from our liability by reason of any such variation or extension being granted to the Vendor or for any forbearance, act or omission on the part of the Company or any indulgence by the Company to the Vendor or by any such matter or things whatsoever which under the law relating to sureties would have the effect of relieving us.
5. We, ... Bank further undertake not to revoke this guarantee during its currency except with the previous consent of the Company in writing.

6. We, ... Bank also agree that the Bank's liability under this guarantee shall not be affected by any change in the constitution of the Vendor or dissolution .....

7. Notwithstanding anything contained herein above:
    i. Our liability under this guarantee shall not exceed Rs.....
    ii. This Bank Guarantee shall be valid upto and including .....; and
    iii. We are liable to pay the guarantee amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before …… (validity + ---weeks from the date of expiry of this guarantee).

8. This Guarantee shall be governed by Indian laws and the Courts at Mumbai, India shall have the exclusive jurisdiction.

IN WITNESS WHEREOF the Bank has executed this document on this..... day of .....

For ..... Bank

(by its constituted attorney)

(Signature of a person authorized to sign on behalf of "the Bank")

NOTE:-

1. Indigenous Vendor or Foreign Vendor through Indian Bank to submit BG.
2. If BG is not received directly from Bank then ECGC Ltd. shall get the Bank Guarantee verified and only on confirmation of verification the Bank Guarantee shall be considered as submitted. Expenses for BG verification shall be borne by ECGC Ltd.

Annexure – 7: Details of Professional staff

Details of Professional staff who will be engaged for the project

(pre-Implementation, during Implementation and post Implementation during O & M)

(Separate Sheet for every Staff member that is likely to be involved in the project)

1. Name of Employee
2. E-mail Id
3. Phone No. (Office)
4. Mobile No
5. Date since working in the Firm
6. Professional Qualifications
7. Experience

Sr. No.	Details of similar work/ services undertaken	Brief Details of services undertaken in India/abroad and the Organization where assignment was undertaken	Period: From-To
01			
02			
03			
04			

Annexure – 8: Queries Format

Sr No	Bidder Name	Page No (tender Ref)	Clause (tender Ref)	Description in the tender (tender Ref)	Query
1					
2					

Note: The queries may be communicated only through the e-mail id provided, it-tender@ecgc.in. Responses of queries will be uploaded on ECGC website or emailed to concerned bidder. No queries will be accepted on telephone or through any means other than e-mail. The queries shall be sent in .xls/.xlsx format in the above mentioned proforma.

Annexure – 9: Format for Letter of Authorization
(To be submitted on the Bidder's letter head)

To

The Deputy General Manager (Information Technology)
ECGC Ltd
Information Technology Division,
The Metropolitan,
7th Floor, C-26/27,
E Block, Bandra-Kurla Complex,
Mumbai-400051.

Letter of Authorisation for Attending Bid Opening for Tender Ref: ECGC/Tender-03/IT/08/2024-25

The following persons are hereby authorized to attend the bid opening on _____(date) in the tender for **"REQUEST FOR PROPOSAL FOR APPOINTMENT OF SYSTEM INTEGRATOR (SI) FOR (SUPPLY AND IMPLEMENTATION) SETTING UP OF DISASTER RECOVERY CENTRE FOR ECGC LIMITED** on behalf of M/S_____ (Name of the Bidder) in the order of preference given below:

Order of Preference Name Designation Specimen Signature

I

II

(Authorized Signatory of the Bidder)

Date_____

(Bidder's Seal)

1. Maximum of two persons can be authorized for attending the bid opening.
2. Permission for entry to the hall where bids are opened may be refused in case authorization as prescribed above is not submitted.

3. Please note that bid opening shall be done in the presence of ECGC Auditors following internally laid down audit process of the Company.

Annexure - 10: Non-Disclosure Agreement Format

This confidentiality and non-disclosure agreement is made on the.....day of....., 20....

BETWEEN

_____(Bidder), (hereinafter to be referred to as Bidder/Receiving Party which expression shall unless repugnant to the subject or the context mean and include its successors, nominees or assigns a company incorporated under the Companies Act, 1956/Indian Companies Act, 2013, or a firm registered under LLP Act, 2008/Indian Partnership Act, 1932 and having its principal office at .....(address).

AND

ECGC LIMITED (hereinafter to be called "ECGC") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns having its Registered Office at ECGC Bhawan, CTS No.393,393/1 to 45, M.V Road, Andheri East, Mumbai – 400069, ECGC Bhawan, CTS No.393,393/1 to 45, M.V Road, Andheri East, Mumbai – 400069, Maharashtra on the following terms and conditions:

WHEREAS, in the course of the business relationship between the aforesaid parties, both the parties acknowledge that either party may have access to or have disclosed any information, which is of a confidential nature, through any mode and recognize that there is a need to disclose to one another such confidential information, of each party to be used only for the Business Purpose and to fulfill the requirements of ERM and to protect such confidential information from unauthorized use and disclosure;

NOW THEREFORE, in consideration of the mutual promises contained herein, the adequacy and sufficiency of which consideration is hereby acknowledged and agreed, the parties hereby agree as follows: —

This Agreement shall apply to all confidential and proprietary information disclosed by one party to the other party, including information included in the caption 'Definitions' of this Agreement and other information which the disclosing party identifies in writing or otherwise as confidential by the disclosing party to the receiving party. ("Confidential Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, electronically or through visual observation or by any other means to one party (the receiving party) by the other party (the disclosing party).

1. Definitions

(a) CONFIDENTIAL INFORMATION means all the information of the Disclosing Party which is disclosed to the Receiving party pursuant to the business arrangement whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, inventions, techniques, processes, plans, algorithms, software programs, source code, semiconductor designs, schematic designs, business methods, customer lists, contacts, financial information, sales and marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs, operations, strategies, inventions, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription lists, customer lists, photo files, advertising materials, contract quotations, charity contracts, documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, statistics, facts, figures, numbers, records, professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barristers, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors, Surveyors, Loss Assessors, Investigators, Forensic experts, Scientists, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Indian Evidence Act, 1872, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defences taken before a Court of Law, Judicial Forum, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Disclosing Party.

The above definition of Confidential Information applies to both parties equally; however, in addition, without limitation, where the Disclosing Party is the ECGC, no information that is exempted from disclosure under section 8 or any other provision of Right to Information Act, 2005 shall at any time be disclosed by the Receiving Party to any third party.

(b) MATERIALS mean including without limitation, documents, drawings, models, apparatus, sketches, designs and lists furnished to the Receiving Party by the Disclosing Party and any tangible embodiments of the Disclosing Party's Confidential Information created by the Receiving Party.

2. Covenant Not to Disclose

The Receiving Party will use the Disclosing Party's Confidential Information solely to fulfill its obligations as part of and in furtherance of the actual or potential business relationship with the Disclosing Party. The Receiving Party shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Disclosing Party or its subsidiaries or affiliates, and shall not

disclose the Confidential Information to any unauthorized third party. The Receiving Party shall not disclose any Confidential Information to any person except to its employees, authorized agents, consultants and contractors, on a need to know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms as restrictive as those specified in this Agreement.

In this regard, any agreement entered into between the Receiving Party and any such person/s shall be forwarded to the Disclosing Party promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the Receiving Party shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information. The Receiving party shall use the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information, and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use. In no event shall the Receiving Party take all reasonable measures that are lesser than the measures it uses for its own information of similar type. The Receiving Party and its Representatives will immediately notify the Disclosing Party of any use or disclosure of the Confidential Information that is not authorized by this Agreement. In particular, the Receiving Party will immediately give notice in writing to the Disclosing Party of any unauthorized use or disclosure of the Confidential Information and agrees to assist the Disclosing Party in remedying such unauthorized use or disclosure of the Confidential Information.

The Receiving Party and its Representatives shall not disclose to any person including, without limitation any Company, sovereign, partnership, company, Association of Persons, entity or individual-

(i) the fact that any investigations, discussions or negotiations are taking place concerning the actual or potential business relationship between the parties,
(ii) that it has requested or received Confidential Information, or
(iii) any of the terms, conditions or any other fact about the actual or potential business relationship.

This confidentiality obligation shall not apply only to the extent that the Receiving Party can demonstrate that:
(a) the Confidential Information of the Disclosing Party is, or properly became, at the time of disclosure, part of the public domain, by publication or otherwise, except by breach of the provisions of this Agreement; or
(b) was rightfully acquired by the Receiving Party or its Representatives prior to disclosure by the Disclosing Party;
(c) was independently developed by Receiving Party or its Representatives without reference to the Confidential Information; or

(d) the Confidential Information of the Disclosing Party is required to be disclosed by a Government agency, is the subject of a subpoena or other legal or demand for disclosure; provided, however, that the receiving party has given the disclosing party prompt written notice of such demand for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order prior to such disclosure.
(e) is disclosed with the prior consent of or was duly authorized in writing by the disclosing party.

3. Return of the Materials

Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information received as Confidential Information or shall certify to the disclosing party that all media containing such Information have been destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the receiving party's counsel, solely for the purpose of proving the contents of the Information.

4. Ownership of Confidential Information

The Disclosing Party shall be deemed to be the owner of all Confidential Information disclosed by it or its agents to the Receiving Party or its agents hereunder, including without limitation all patents, copyright, trademark, service mark, trade secret and other proprietary rights and interests therein, and Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as granting any rights to the Receiving Party, by license or otherwise in or to any Confidential Information. Confidential Information is provided “as is” with all faults.

By disclosing Information or executing this Agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this Non-Disclosure Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

5. Remedies for Breach of Confidentiality

1. The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors or agents) and that any unauthorized disclosure of any

Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent or mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

2. The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

6. Term

This Agreement shall be effective on the first date written above and shall continue in full force and effect at all times thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind the parties, and also their successors, nominees and assignees, perpetually.

7. Governing Law & Jurisdiction

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of law provisions. Any proceedings arising out of or in connection with this Agreement shall be brought only before the Courts of competent jurisdiction in Mumbai.

8. Entire Agreement

This Agreement sets forth the understanding between the parties as to the subject-matter of this Agreement and supersedes all prior representations, discussions, and negotiations whether oral or written or electronic. This Agreement may be amended or supplemented only in writing that is signed by duly authorized representatives of both parties.

9. Waiver

No term or provision hereof will be considered waived by either party and no breach excused by the Disclosing Party, unless such waiver or consent is in writing signed by or on behalf of duly Constituted Attorney of the Disclosing Party. No consent or waiver whether express or implied of a breach by the Disclosing Party will constitute consent to the waiver of or excuse of any other or different or subsequent breach by the Receiving Party.

10. Severability

If any provision of this Agreement is found invalid or unenforceable, that part will be amended to achieve as nearly as possible the same economic or legal effect as the original provision or will be struck off and the remainder of this Agreement will remain in full force.

11. Notices

Any notice provided for or permitted under this Agreement will be treated as having been given when (a) delivered personally, and/or (b) sent by confirmed telecopy/fax, and/or (c) sent by commercial overnight courier with written verification of receipt, and/or (d) mailed postage prepaid by certified or registered mail, return receipt requested, and/or (e) by electronic mail, to the party to be notified, at the address set forth below or at such other place of which the other party has been notified in accordance with the provisions of this clause. Such notice will be treated as having been received upon actual receipt.

ECGC Ltd.: For letter- Through post

Deputy General Manager,

RMD

ECGC Limited

4th floor, ECGC Bhawan,

CTS No 393 M V Road Andheri (East) Mumbai 400069

For email: rmd@ecgc.in

(Name and Adress of the bidder)

For email; _____ (email id of the bidders)

IN WITNESS WHEREOF THE PARTIES HERE TO have set and subscribed their respective hands and seals the day and year herein above mentioned.

a) SIGNED SEALED & DELIVERED BY THE WITHIN NAMED ECGC Ltd.

_____

In the presence of

Witness : 1_____

Witness: 2_____

b) SIGNED SEALED & DELIVERED BY THE WITHIN NAMED BIDDER

In the presence of

Witness: 1_____

Witness: 2_____

Annexure 11: Technical Bid Score Sheet Format

Each Bidder will be evaluated on the scale of 100 marks on various technical parameters as below. The Technical bid will have a weightage of seventy marks and thirty marks are fixed for financial bid.

Sr. No.		Weightage	Breakup
A	SI Capabilities (as per Qualification Criteria Scoring)	100	
B	Server Specification	200	
C	Storage Specifications	100	
D	Virtualisation Specifications	100	
E	Data Centre Security & Nw Solution	150	
1	UTM		40
2	Server load balancer, WAF & GSLB		30
3	Internal Firewall		20
4	Datacentre Switch		30
5	TOR Switch		10
6	Server Security		10
7	DAM		10
F	Replication Software	50	
G	Overall Solution	100	
	Total Score	800	

Annexure – 12 - CODE OF INTEGRITY DECLARATION

I/We working as in (name of the Bidder and its address in full be mentioned), hereby solemnly affirm and declare that I/We have been authorized by the firm/Company to sign the bids. I/We, hereby declare and certify, on behalf of the firm/Company, that we have accepted all the terms & conditions mentioned in the ……and we shall abide by all the terms & conditions of RFP/Agreement.

I/ We hereby agree and undertake that we have not directly or through any other person or firm offered, promised or given nor shall we offer, promise or give, to any employee of ECGC involved in the processing and/or approval of our proposal/offer/bid/contract or to any third person any material or any other benefit which he/she is not legally entitled to, in order to obtain in exchange advantage of any kind whatsoever, before or during or after the processing and/or approval of our proposal/offer/bid/contract.

I/we further declare that in relation to my/our Bid submitted to ECGC, in response to RFP NO……,I/we…….hereby undertake that I/we shall abide by the Code of Integrity and make disclosure as to any Conflict of Interest at all times, and understand that any breach of the Code of Integrity will render me/us liable to be removed from the list of registered bidders, and would also subject me/us to other punitive and penal actions such as, but not limited to, cancellation of contracts, banning, debarring and blacklisting or action in the court of Law, and so on.

Signature of Authorized Signatory of the Bidder with Seal & Stamp

Date: Place:

Name:

Contact No (Mobile):

Email Id: