(A Government of India Enterprise)

You focus on exports. We cover the risks.

REQUEST FOR PROPOSAL

FOR

APPOINTMENT OF SYSTEM INTEGRATOR (SI) CUM MANAGED SERVICES PROVIDER (MSP)

FOR SUPPLY, IMPLEMENTATION AND MAINTENANCE OF DATA CENTRE SETUP AND CLIENT-SIDE INFRASTRUCTURE

FOR

ECGC'S SMILE PROJECT

Ref: ECGC/Tender-02/IT/03/2020-21

Date: 05.03.2021

Index

Table of Contents

Section 1

1. Introduction

1.1. Invitation to Bidders

By way of 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'), a company wholly owned by Government of India and set up in 1957, invites competitive Bids from vendors (hereinafter referred to as ('**the Bidder(s)**'.) for **"APPOINTMENT OF SYSTEM INTEGRATOR (SI) CUM MANAGED SERVICES PROVIDER (MSP) FOR SUPPLY, IMPLEMENTATION AND MAINTENANCE OF DATA CENTRE SETUP AND CLIENT-SIDE INFRASTRUCTURE FOR ECGC'S SMILE PROJECT"**

The "Technical and Price/Commercial 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 www.ecgc.in. 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**

Bid Document Availability	The Bid Document can be downloaded from website up to 26.03.2021.
Submission of Bidder's Queries (in format given in tender document) before Pre-bid	03:00 pm 12.03.2021
Pre-Bid meeting	10:00 AM on 19.03.2021.
Last date of submission of Bids	1:00 PM on 26.03.2021.
Opening of Sealed Bids	The bids will be opened as per internally laid down Audit process of ECGC.
Solution Presentation by Bidder	Date and time shall be intimated later.
Opening of Price/Commercial Bids	Within fifteen days of opening of Technical Bids.
Contact Details: Deputy General Manager (Information Technology) : 022-6144 8155 Assistant General Manager (Information Technology) : 022 -6144 8153 Senior Manager (Information Technology) : 022 – 6144 8168 Assistant Manager (Information Technology) : 022 – 6144 8145	
Address for Communication and submission of Bid.	Deputy General Manager (Information Technology) ECGC Limited, Information Technology Division, The Metropolitan, 7th Floor, C – 26/27, E Block, Bandra-Kurla Complex, Mumbai – 400 051
Telephone	022-6144 8153/68/45
All correspondence / queries relating to this RFP Document should be sent to / through following email ID only	it@ecgc.in

Section - 2

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

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://www.ecgc.in 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, 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.

3.1.8 Bids shall be submitted in three parts i.e. (1) Qualification/ Eligibility Bid (2) Technical Bid and (3) Price/Commercial 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 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 E)** and the same shall be submitted along with Eligibility Bid in the same envelop.

3.1.11 The Bidder shall submit the Price/Commercial Bid as per the form provided under **Annexure – 5 (A to C)** and the same shall be enclosed in another sealed envelope.

3.1.12 Supporting documents are to be submitted in the Qualification, Technical as well as Price/Commercial 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. Validity Period:

Bids shall have the validity period of 90 days from the closing date of the RFP. 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.

3.4. Scope of Work for System Integrator (SI) cum Managed Service provider (MSP)

ECGC has been in the process of rolling out its newly developed ERP system named as 'SMILE Software'. ECGC wishes to appoint a System Integrator company for procuring, implementing and managing the Infrastructure for SMILE System on turn-key basis for five years period. The scope of work broadly includes following:

(1.) The SMILE System requires implementing a UAT environment along with setting up a full-fledged Primary Data center (PDC) at Mumbai.

(2.) SI will be required to propose a primary data center site as per the specifications given for the data center in the tender document. **(Annexure –4 A)**

(3.) SI needs to setup the data center incorporating the Space, Rack, cooling etc. requirements for the BOM requested for setting up the private cloud of ECGC's SMILE Project.

(4.) The hardware requirements for UAT and PDC environment as per internal sizing done, is given as a part of tender document (Annexure – 4. B to E).

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

(6.) The project needs to be rolled out as per the timelines to be shared with interested bidders.

(7.) The prioritized implementation of UAT setup is to be completed by May 2021.

(8.) ECGC will be free to change the quantities of Bill of Material based on UAT results and SI will be accordingly issued the fresh/ modified/ additional order (s) for DC setup.

(9.) The devices and hardware provisioned shall be under 5 years post deployment warranty support from OEM.

(10.) SI will be required to setup Microsoft Active Directory environment. ECGC is currently using Microsoft Active Directory - 2012. SI will be required to do the gap-analysis, design, implement and migrate the existing AD setup to new AD. The hardware and software licensing requirement for the same should be quoted as line item.

(11.) ECGC is currently using Zimbra as the mailing solution. SI will be required to propose, design and implement a new mailing solution including migration of mail boxes, user PSTs, migration of journals from old Microsoft exchange and Zimbra backups. SI will be required to implement an on-premise mail archival solution. The hardware and software licensing requirement for the same should be quoted with solution.

(12.) ECGC is looking for implementation of DDI (DHCP + DNS Security + IPAM) solution for managing the IP addresses. Also DNS security for all the DNS entries must be done.

(13.) SI will be required to migrate existing portal servers, Investment servers, SMTP, proxy etc. to new setup. The current sizing of these servers would be shared with prospective bidders.

(14.) SI will be required to provide day-to-day managed services for infrastructure environment of Data center (PDC, NDC, DR) and branch offices for all ECGC's locations across India as **'Managed Services Provider (MSP)'**. The Primary Data Centre and DR environment will be as per the specification given in the tender document.

(15.) The NDC and DR implementation is not in current scope of this tender and will be implemented in due course of time through separate tendering / ordering process. (However, the MSP services for Infrastructure include PDC, NDC and DR sites management including other ECGC office's setup and selected SI shall onboard and strengthen the team, if required as per the mutually agreed timelines).

(16.) The initial minimum resources requirement to manage the limited Infrastructure of UAT (to begin with) shall be proposed as a part of the proposed solution.

The resource strengthening as per Data Center and other services Go-live timelines shall be mutually planned with ECGC. SI shall provide resource-wise /service wise managed services costing till full-fledged resources onboarding is done. The SI's MSP team will be required to ensure smooth transition of Data Center and end-user services from current MSP team.

(17.) The selected SI will be required to draw a detailed SOW with SLAs for SI and MSP scope and enter into agreement with ECGC.

(18.) SI shall elaborate the support structure for P1, P2, P3 calls and plan for deputing onsite resources as dedicated or shared across onsite services.

(19.) 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) Hiring a Data Centre on co-location model as per the specifications given. Installation, commissioning of Data Centre components.

(v) Provisioning any additional resources required

(vi) The SI shall have back-to-back arrangement with OEM to meet infra scalability requirement on request.

(vii) Coordinating with different vendors (new or existing) during UAT and Data Centre implementation.

(viii) End-to-end testing of data center equipment.

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

(20.) The indicative list of services as MSP are given under:

Brief description of setup:

The SMILE software under implementation will have a primary data centre (PDC), hosting development, UAT and production environment (implementation under SI's scope). The NDC and Far DR will be implemented in due course of time. The Data Centre environment will be as per the specification given in the tender document.

ECGC has presence in around 50 locations across the country. ECGC branches are connected using a MPLS VPN, and this network, including and up to CE routers is managed by the network provider. ECGC employees (~650) normally work on Windows PCs (Win 10) and Laptops (Win 10). ECGC has deployed ~700 PCs and ~150 Laptops. ECGC employees also access mail on mobile (Android / iOS), and iPads and Android tablets. Each employee is normally provided with a printer / B&W MFD / Colour MFD. Standard user software like MS Office, PDF reader, web browsers, device drivers, mail client, bilingual software / fonts etc. are provided to all employees. Special software is also provided to few users as per need. List of ECGC locations required to be supported (remotely or onsite) is available at the following URL: https://www.ecgc.in. The updated list will be shared with interested bidders.

i.) <u>Helpdesk</u>

(a) The centralized helpdesk shall be set up onsite at ECGC Express Towers office (this may be shifted to BKC or Andheri building of ECGC when functional), and shall include all user calls like

1. PC and Printer configuration,
2. Mail configuration,
3. Proxy and AD settings configuration,
4. Installing, uninstalling and reinstalling software,
5. PST handling,
6. Backups and restoration of data on user request.
7. User Assistance
8. Install the software updates and upgrades

(b) These calls are to be attended by engineer visit in ECGC, Express Towers, Nariman Point, Mumbai premises. For other locations, helpdesk may use remote login services, followed by engineer visits as required.

(c) At major remote locations viz. Bandra (Mumbai), Delhi, Kolkata, Chennai, Bengaluru, Hyderabad, Tirupur, and Ahmedabad each at least one engineer must be posted. This engineer shall report to the centralized helpdesk, and shall be responsible for the entire region i.e. including physical visits to all branch locations attached to the region as required.

(d) The centralized helpdesk shall also provide priority service to 10 ECGC Senior Management (list shall be shared with successful bidder) employees, for whom all calls shall be classified as P1.

(e) SLA: For P1 calls, resolution time required is two hours. For all other calls (P2) resolution time required is four hours.

(f) The estimated number of monthly Infra support calls will be between 800 - 1200 approx.

(g) The support Window for normal issues should be 9.00 am to 06.00 pm but for critical issues it will be 24*7 (such as Server issues/ planned or unplanned Activities etc.)

(h) MSP Team shall provide minimum support on holidays (as per ECGC's region-wise/ branch-wise Holiday list) of respective locations either from HO or from a remote support location. The requirement will be shared to the onsite program manager on case to case basis.

ii.) <u>System Administration</u>

(a) First layer support for the HCI Nodes and other Physical servers along with the virtualization layer at the DC and DR should be provided by the System Admin. The Bidder shall be required to manage the server, OS and applications on all the servers beyond the base OS.

(b) Bidder shall be required to perform all System Administration tasks like configuration, monitoring, backup and archival, restoration, installation / uninstall / reinstallation, license and support management, performance optimization, hardening, interfacing with application teams for issue resolution etc.

(c) Bidder shall also be required to manage other servers installed at the different offices of ECGC (located in Mumbai).

(d) Bidder shall also have to manage the WSUS server and patch management services driven through it for servers as well as user machines.

(e) Bidder shall also have to manage the ECGC Windows Active Directory (multiple servers, including those deployed at remote locations).

(f) Install the software updates and upgrades

(g) SLA: All calls to be considered as P1 calls, and resolution time required is two hours.

iii.) Mail Management

(a) Bidder shall be required to manage the entire mail setup of ECGC which is currently on Zimbra or the new setup proposed and implemented as a part of tender scope. The below mail management services shall then be read; as applicable for new mailing solution.

(b) This will include user issues which cannot be handled by helpdesk engineers, mail server administration, backup, restoration, journal management (including old journals from MS Exchange), archival, user or distribution list creation / deletion / activation / deactivation / provisioning / Quota / PSTs, Zimbra LDAP, password management, Zimbra HSM, Advanced search, Calendar, Briefcase, Tasks, Zimlets, Log management, review, and archival, and providing delivery reports, Command Line interface, SSL certificates, MTA, Custom retention, litigation hold, real-time backup / restore, one-click DR recovery, compression, dedup, HA, UC integration, 2FA, policy management, archiving and discovery, upgrades, updates, license management, spam filter, interfacing with OEM / ISV / Data Center provider, underlying Linux OS etc. at both DC and DR.

(c) The scope will also include managing the IMSS spam filter and SMTP services including managing the quarantine, monitoring the queue, releasing genuine messages, blocking / unblocking mail domains etc.

(d) SI will have to manage and integrate the Smile project with Zimbra (existing mailing solution) till new Mailing solution is made live. Once new mailing solution is implemented, SI shall ensure smooth transition to same.

(e) SLA: For P1 calls, resolution time required is two hours. For all other calls (P2), resolution time required is four hours.

iv.) Antivirus Management

(a) The Bidder shall be required to manage the primary Antivirus server located in the Data Center, and secondary AV servers deployed in the remote locations, and the AV clients installed on the servers and user machines.

(b) SLA: 100% compliance on version, 99% compliance on definition, 99% compliance on scan, Virus / malware alert to all ECGC users within two hours of outbreak.

v.) Asset Management, Call logging / monitoring, and SLA monitoring

(a) ECGC has deployed an asset management tool, which keeps the records of the assets (IT & Non-IT) the bidder shall have to manage and ensure asset inventory match with ERP records. The shared/ dedicated resource will be responsible for coordinating with ECGC offices and update/ reconcile with past, present and any new asset inventory including generating and sending bar codes to such locations.

(b) Bidder shall have to deploy resources for using the asset inventory / call logging / SLA monitoring solution deployed by ECGC for issue management / resolution and MIS, which shall form basis of SLA measurement.

(c) SLA: NA (However, continued non-compliance / non-conformity / deviation may result in invocation of bank guarantee and / or termination of contract.)

vi.) <u>Vendor Management</u>

(a) The Bidder shall be required to maintain the list of and manage all third-party vendors of ECGC, for L2 or higher support, call logging, license installation, certificate configuration, escalations, AMC / Warranty, follow ups etc.

(b) The Bidder shall coordinate with vendors in case of any planned / unplanned activity to be carried out, and shall monitor the activity thereof until completion.

(c) The Bidder shall be required to interact with users of ECGC and issue asset card to every employee once a year.

(d) SLA: NA (However, continued non-compliance / non-conformity / deviation may result in invocation of bank guarantee and / or termination of contract.)

vii.) <u>Project Management</u>

(a) The vendor shall appoint a project manager to the onsite location, who shall be responsible for managing his team, and the SLA.

(b) The PM shall be required to submit a service availability report at BOD and EOD for all ECGC services under the Bidder’s management.

(c) The PM shall be required to submit weekly pending and completed reports for both his team and those escalated to vendors.

(d) The PM shall also be required to submit an incident report within four hours of an incident, even if the issue is unresolved. The PM shall be further required to submit a comprehensive incident report with RCA within 24 hours of issue resolution.

(e) The PM shall conduct monthly review meeting with ECGC team and provide Executive Summary as well as performance analysis reports for the Bidder's team.

(f) SLA: NA (However, continued non-compliance / non-conformity / deviation may result in invocation of bank guarantee and / or termination of contract.)

viii.) Security Monitoring and Management

(a) ECGC is having an in-house SOC implementation.

(b) SI team shall be required to set up a 24*7 remote SOC monitoring for the new setup in the DC and DR, and also for monitoring messaging security, content filtering, Proxy server, Antivirus, and other security apparatus as may be added in future.

(c) SI's team shall be required to carry out day to day activities on the Firewall such as opening and closing of ports, specific or AD-HOC firewall rule requirements etc.

(d) SI's team shall be required to set up a 24*7 security helpdesk for user / administrator issues regarding for blocking / unblocking, blacklisting / whitelisting, mail quarantine / mail release, delivery and failure reporting, user provisioning / de-provisioning etc.

(e) SI's team shall be responsible for troubleshooting / configuration changes on the servers, and also shall be responsible for interfacing with OEM / ISV for support, license installation / reinstallation, version change / upgrade, software installation / uninstallation etc.

(f) Si's team shall be responsible for installing, reinstalling, and configuring SSL certificates on to all servers as required by ECGC.

(g) SLA: All calls to be considered as P1 calls and resolution time required is two hours.

ix.) MSP Services Penalty

(a) Penalty for SLA violation of P1 calls shall be 0.01% per violation of the total order value of five years for MSP services.

(b) Penalty for SLA violation of P2 calls shall be 0.01% per violation of the total order value per quarter.

(c) If the total penalty applicable in a quarter exceeds 1% of the total order value per quarter, penalty applicable in the subsequent quarter shall be calculated as double of actual value of applicable penalty in that quarter.

(d) If the total penalty applicable in any quarter exceeds 5% of the total order value per quarter, ECGC reserves the right to charge the penalty, invoke the performance bank guarantee over and above the penalty, and terminate the contract with a notice period of three months.

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

3.5. The bidding documents

3.5.1 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 E)

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

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

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.

3.5.2 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. Not more than 3 participants will be allowed from each bidder company.

The queries shall be communicated only through the e-mail id provided, IT@ecgc.in the format provided in Annexure -8.]

ECGC would issue clarifications/ Amendments in writing via e-mail and will become part of RFP.

3.6. Preparation of bids

3.6.1 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.

3.6.2 Documents Comprising the Bid

3.6.2.1 Documents comprising the Eligibility and Technical Bid envelope 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 Form as per Annexure-1 and Annexure – 4 (A to E)

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

3.6.2.2 The papers like Forms, supporting documents as mentioned above etc. should be submitted in one lot in one envelope.

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

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

3.6.3 Price / Commercial Bid

3.6.3.1 Each Bidder is required to complete a Price/Commercial Bid Envelope, comprising of the Price/Commercial Bid Form as per Annexure – 5 (A to C) on the letter head of the Bidder.

3.6.4 Bid Form

The Bidder shall complete both the aforesaid Envelopes containing the Technical and Price/Commercial Bids, along with the requisite documents wherever mentioned and submit them simultaneously to the Company in a single outer envelope. Bids are liable to be rejected if all Bids (Eligibility, Technical Bid and Price/Commercial Bid) are not received together.

3.6.5 Bid Prices

3.6.5.1 Prices are to be quoted in Indian Rupees only.

3.6.5.2 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.

3.6.5.3 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.

3.6.6 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.

3.6.7 Partial bids

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

3.6.8 Period of Validity of Bids

3.6.8.1 Bids shall remain valid for a period of 60 days from the date of opening of the Bid.

3.6.8.2 In exceptional circumstances, the Company may solicit the Bidder's consent to an 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.

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

3.6.9 Format and Signing of Bid

3.6.9.1 **Each Bid shall be in three parts:**

Part A – Eligibility Bid

Part B - Technical Bid.

Part C– Price/Commercial 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/Commercial Bid" as the case may be.

3.6.9.2 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.

3.6.9.3 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.

3.6.9.4 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.

3.6.9.5 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.

3.6.9.6 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.

3.6.9.7 GLOSSARY: 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.

3.7. Submission of bids

3.7.1 Sealing and Marking of Bids

3.7.1.1 The Bidder(s) shall seal the NON-WINDOW envelopes containing one copy of “Technical Bid” and one copy of “Price/Commercial Bid” separately and both 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).

3.7.1.2 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.

3.7.1.3 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

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

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

3.8. Deadline for Submission of Bids

3.8.1 Bids must be received by the Company at the address specified, no later than the date & time specified in the “Schedule of Events” in Invitation to Bid.

3.8.2 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.

3.8.3 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.

3.9. Late Bids:

Any Bid received after the deadline for submission of Bids prescribed, will be rejected, and subsequently destroyed. No Bids shall be returned.

3.10. Modification and Withdrawal of Bids

3.10.1 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.

3.10.2 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.

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

3.10.4 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.

3.11. Opening and evaluation of bids

3.11.1 Opening of Bids by the Company

3.11.1.1 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.

3.11.1.2 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.

3.11.1.3 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.

3.11.2 Preliminary Evaluation

3.11.2.1 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.

3.11.2.2 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.

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

3.11.2.4 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.

3.11.3 Evaluation of Bids

3.11.3.1 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.

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

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

3.11.3.4 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.

3.11.3.5 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 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.

3.11.3.6 The Bidders submitting bids in accordance of tender 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.

3.11.3.7 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.

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

3.11.4. Evaluation of Price Bids and Finalization

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

3.11.4.2 The Price/Commercial Bid will be scored on a total of 100 as under:

Cs = (Cmin / Cb) x 100 where,

Cs = Commercial score of the Bidder under consideration

Cmin = Lowest Price/Commercial Bid quoted

Cb = Price/Commercial Bid under consideration

3.11.4.3 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)
- Weight of 30% to the commercial score

Combined Technical and Commercial Score, calculated up to two decimal points, will be as under:

Bs = (0.7) * Ts + (0.3) * Cs

Where,

Bs = overall combined score of Bidder under consideration

Ts = Technical score of the Bidder under consideration

Cs = Commercial score of the Bidder under consideration

3.11.4.4 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.

3.11.4.5 Company reserves the right to reject any or all incomplete Bids.

3.11.4.6 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.

3.11.4.7 The queries may be communicated only through the e-mail id provided, IT@ecgc.in the format provided in Annexure 8.

3.11.4.8 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.

3.11.5 Contacting the Company

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

3.11.5.2 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 barring from any future RFPs / contracts / business with ECGC.

3.11.6 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 that had high 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

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

3.11.7.1 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.

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

3.11.8 Performance Bank Guarantee

3.11.8.1 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 - 5 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.

3.11.8.2 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.

3.11.8.3 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.

3.11.8.4 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.

3.11.9 Earnest Money Deposit:

Earnest Money Deposit (EMD) of Rs. 1,00,000 (Rupees One lakh only) is required to be submitted preferably by NEFT. IT 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 favour of '**ECGC Limited'**, payable at Mumbai. EMD deposited by the unsuccessful bidders will be refunded by way of handing over the original Demand Draft/ Bankers Cheque duly endorsed by the Competent Authority of ECGC Limited. EMD of successful bidder will be converted into security deposit which will be returned without any interest after the satisfactory job completion. Under any circumstances, ECGC Limited will not be liable to pay any interest on the EMD.

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 Technical 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;

"The Project" means "**APPOINTMENT OF SYSTEM INTEGRATOR (SI) CUM MANAGED SERVICES PROVIDER (MSP) FOR SUPPLY, IMPLEMENTATION AND MAINTENANCE OF DATA CENTRE SETUP AND CLIENT-SIDE INFRASTRUCTURE FOR ECGC'S SMILE PROJECT"**

4.1.1.7 "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 3.4 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 -3, 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 Damages/ Liability clause.

ECGC reserves the right to deduct from the total contract price to be paid to the BIDDER in such manner in the event of the following:

Reason	Delay of One Week	Delay beyond first week and part thereof
Delay in providing/ensuring deliverables/ services beyond the agreed timeline (delay attributable to the Bidder)	Caution Note	5% of the contract value, and proportionally for the part of the week. Minimum 5%
Inordinate delay in responding to the references made by the ECGC (delay attributable to the Bidder)	Caution Note	5% of the contract value, and proportionally for the part of the week. Minimum 5%

4.1.5 Service Delivery Location

The major scope of work as mentioned above will be required to be delivered at third party Data Centre proposed by SI. However, the Vendor's team would 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 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. The Team may also visit the existing Data Centre and/ or Disaster Recovery locations of ECGC to ascertain the inputs required for drawing out the specifications.

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 Go-Live of UAT environment by May 2021 and DC environment by August 2021.

These will form the basis of delivery timelines. The exact specifications of the timeliness 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 in Mumbai and as per the provisions of the Arbitration and Conciliation Act, 1996 (as amended in 2015). 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 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. Bidder shall protect the Company against any claims thereof.

4.1.17 Intellectual Property Right (IPR)

The Bidder 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.

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

S.No	Activity	Acceptance (YES/NO)	Penalty Terms
1	24 x 7 x 365 online support coverage for hardware / software calls logged.		Rs. 10,000/- per day, maximum up to 5% of MSP value for the respective year
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.		
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 5% of the MSP cost
4	Warranty start date shall be from the product delivery and installation date for the 5 years		
5	Delay in Project Execution: Delay in Project Execution shall attract penalty calculated @0.1% of total PO value per day of delay, maximum up to 5% 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		
6	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 15% of Datacenter quote

****

Section – 5

Annexure – 1: Eligibility Criteria & Specifications

(A) SYSTEM INTEGRATOR'S ELIGIBILITY CRITERIA:

Sr No	Description	Details		Parameters	Marks
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 cost.			
23	Bidders Company should have at least 25-35 years of existence.	<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 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 2020.	< IT returns acknowledgments and / or Audited Financial Statements / statements certified by Chartered Accountants to be provided for last two financial years ended on 31.03.2020 >			Maximum Marks 15
	Turnover between 50,00,00,000/- to 60,00,00,000/-			5	
	Turnover between 60,00,00,001/- to 90,00,00,000/-			10	
	Turnover above 90,00,00,000/- (90 Cr)			15	
26	Bidder should be profitable company with net profit of at least 3% 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 31.03.2020 >			Maximum Marks 15
	Company with net profit of 3 to 5%			5	
	Company with net profit of 6 to 7%			10	
	Company with net profit of 8 to 10%			15	
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 location			3	
	Company with presence in five location			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 in-premise)	<Please attach evidences>		5	Maximum Marks 5

29	The DC Service Provider should be a government organization/ Public sector unit/ Partnership firm / Public Limited Company/ Private Limited Company having its Registered Office in India since last 5-10 years as on 31/03/2021			Maximum Marks 5
	between 5- 10 Years		3	
	10+ Years		5	
30	Bidder should have experience in IT infrastructure and Application development and maintenance and 3-8 customer references for Managed Services for Infra and Application support.	<Please attach evidences, order value, copies>		Maximum Marks 15
	Upto 2 customer reference		1	
	3-5 Customer reference for Apllication and Infra support		7	
	6-8 Customer reference for Apllication and Infra support		10	
	8+ Customer reference for Apllication and Infra support		15	
31	Bidder should have successfully done at least one implementations of HCI 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 HCI Solution implementations		3	
	Bidder with 3-4 HCI Solution implementations		7	
	Bidder with 4+ HCI Solution implementations		10	
32	Bidder Should Have head office in Mumbai	<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	<Please attach evidences, and use separate sheets as necessary>		

	support the proposed product at ECGC			
34	Bidder should produce an Authorization Letter in favour 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>		
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). >		

(B) OEM'S ELIGIBILITY CRITERIA as per Technical specification of HCI nodes given below:

Sr. No.	**Description**	**Details**		
		<Please attach evidences>		
1	OEM Should be in the leaders list of the acceptable industry reports.			
2	Support from the HCI Solution (Hardware + Software) should be from the same OEM.		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 HCI solution should support scaling hyper converged node (compute + storage), compute-only, storage-only (HDDs) independent of each other under a single cluster. Any storage expansion should not include any additional licenses from HCI vendor.		10	10

4	The network switch should support QoS to streamline HCI network traffic to improve traffic filtering, segmentation and performance.		10	10
5	Present scale-out storage to compute only nodes for Seamless failover of compute-only nodes for a fully high available design of HCI		10	10
6	The HCI solution should support connecting to any external 3rd party SAN (FC, ISCSI) and NAS (CIFS, NFS) storage into the HCI cluster for capacity expansion and ease of migration from existing environment to HCI		15	15
7	Min. 4-8* 25Gbps network ports per server node.		5	5
8	The CVM sizing should be done considering expansion to full 64 Nodes and all features of HCI highest license software offered enabled. Document for the same to be attached.		10	10
9	The HCI solution should support various data replication methods 2 mirror data copies, 3 mirror data copies for data protection. Any software license required to enable RF=2 & RF=3 should be quoted from day 1		5	5
10	The HCI solution should support Inline Deduplication across all storage tiers.		5	5
11	The HCI solution should support various data replication methods 2 mirror data copies, 3 mirror data copies for data protection. Any software license required to enable RF=2 & RF=3 should be quoted from day 1		5	5
12	The HCI solution should support Inline Deduplication across all storage tiers.		5	5
		Total		100

Technical Specifications of the HCI Nodes:

S.No	Description	Specification	Compliance (Yes/ No)
1	Form factor	Rack	
2	Size (RU)	1/2	
3	Processor Make	Intel CISC (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	Intel 6240R 2.4GHz/165W 24C/35.75MB DDR4 2933MHz	
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	Disk Controller Ports @12 Gbps	8	
18	Video Controller (support VGA or above resolution)	Yes	
19	Populated Bays (min. 2 internal or more hot plug)	Min. 8	
20	USB Ports (version 2.0/3.0)	2	
21	OS Supported	Windows, Red Hat RHEL or SuSE Linux, CentOS	
22	Network Card Supported	1G, 10G, 25G and above	
23	FC HBA Dual port card / Quad port	1 *CNA with 4 * 10/25Gig Ports - Should support FCoE	
24	Power Management	Screen blanking, hard disk & system idle mode in power on, set up password, power supply surge protected, automatic server reboot	

25	Redundant Power Supply	Redundant platinum grade Power Supplies	
26	Redundant Fan	redundant hot plug system fans	
27	Total No of Ethernet Ports	3x1G, 4x25G SFP	
28	Server scalability to be achieved within the box without adding nodes	Yes	
29	RoHS Compliance	Yes	
30	Max. power consumption of the system (Watt)	800	
31	Availability of the type test report from Central Government / NABL / ILAC accredited laboratory covering verification of all features & functional parameters & environmental tests sequence. Availability of the type test report from Central Government / NABL / ILAC accredited laboratory covering verification of all features & functional parameters & environmental tests sequence.	Yes	
32	Dry heat: test - for 16 hrs at 45 deg C as per IS: 9000/pt-3/sec-5/1977 b) Cold test - for 4 hrs at 0 deg C as per IS: 9000/pt-2/sec-4/1977 c) Damp Heat Cyclic Test - for 2 cycles of 24 hrs at 40 deg C & 95% RH as per IS: 9000/pt-5/sec-1/1981		
	server shall be checked for all the parameters before conditioning, After completion of the above environmental tests sequence, with a recovery period of 1 to 2 hrs, the server shall be functional		
33	Power Supply	230 +/- 10%Vac9652	
34	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.	
35	Certification/Compliance	Supports & Compatible with offered HCI Solution	
36	Support for high availability clustering and virtualization	Yes	

.....

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Annexure – 2 : Bank Details

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 Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 3: Acknowledgement

Date:

To,
Deputy General Manager
Information Technology Division,
ECGC Limited,
The Metropolitan, 7th Floor,
C-26/27, E Block, BKC,
Mumbai - 400051

Dear Sir/Madam,

Subject: Response to the Request for Proposal for "APPOINTMENT OF SYSTEM INTEGRATOR (SI) CUM MANAGED SERVICES PROVIDER (MSP) FOR SUPPLY, IMPLEMENTATION AND MAINTENANCE OF DATA CENTRE SETUP AND CLIENT-SIDE INFRASTRUCTURE FOR ECGC'S SMILE PROJECT"

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 Company

(Company Seal)

Name :

Designation :

Contact No (Mobile) : Email ID :

Annexure – 4A: Technical Solution Requirements of Datacenter Provider

S.NO	Item Description	Compliance (Yes/No)	Documents to be submitted
1	The DC/DR/Cloud Service Provider should be a government organization/ Public sector unit/ Partnership firm / Public Limited Company/ Private Limited Company having its Registered Office in India since last 10 years as on 31/03/2021.		Copy of certificate of incorporation to be provided
2	The DC/DR/Cloud Service Provider should be within the radius of 13 KM of the proposed ECGC office in Andheri		Data Centre location to be provided
3	The DC/DR/Cloud Service Provider must possess below listed certifications for Proposed Datacenters • ISO- 27001:2013 (ISMS) • ISO-20000-1:2011 (ITSM) • ISO-9001:2015 (QMS) • ISO 22301:2012 (BCMS) • ISO 27017 (Cloud Security) • ISO 27018 (Cloud Privacy) • PCI-DSS v3.2.1 • CERT-In Empanelment • Service Organization Controls (SOC) 1 Type 2 Report • Service Organization Control (SOC) 2 Type 2 Report • TIA- 942 Tier- 3 for proposed Data Centre		Copies of unexpired certificates needs to be submitted
4	DC/DR/Cloud Service Provider must have been owning and managing at least Six Data centers in different seismic zones in India from the last Five years		Self-Declaration with details
5	The Proposed Data Center(s) should comply with Tier III standards		Tier III Certificate/Self Certification for Tier III Compliance
6	The DC/DR/Cloud Service Provider should have a minimum Average Turnover of Rs. 550 Crores in the last three financial years from India operations		Balance sheets and P&L Statements

7	The DC/DR/Cloud Service Provider should have made operating profits in the last three financial years.		Balance sheets and P&L Statements
8	The DC/DR/Cloud Service Provider should be providing Cloud Services to at least 5 PSUs or Central or State Govt. customers as on date of bid submission as per MeitY / Government Community Cloud(GCC) Standards		Work Order Copy / Self Declaration signed by Authorized Signatory / Client Reference Letter
9	The CSP should have provided SAP Cloud Hosting services at any of the their Data centres in India for a minimum period of one year during last five years ending 30.01.2020 as below; At least one work (or multiple work orders from same customer) of value not less than 10 lacs annual billing in a multi-year contract.		
10	The bidder should hold a certificate with a title “SAP-Certified provider of Cloud and Infrastructure Operations” issued by SAP.		Copy of certificate valid as on date of submission of bid
11	The DC/DR/Cloud Service Provider should have a minimum of 5 ISPs already present at the time of Bid		
12	The DC/DR/Cloud Service Provider must not have been black listed by any Government organization or Govt. agency or Banks in India. (A self-declaration signed by the authorized Signatory to be enclosed).		Self-Declaration
13	The proposed Datacenter facility for DC/DR/Cloud Services should be a Carrier Neutral facility		Provide Specifications of Proposed Data center(s)
14	The proposed Datacenter facility for DC/DR/Cloud Services should be in an independent standalone building either		Self-Declaration or Lease/Ownership

	owned by the Datacentre Service Provider or on lease as per local Govt. norms		Agreement
15	DC/DR/Cloud Service Provider Should be providing 24x7x365 shared/dedicated NOC for clients with the help of skilled & certified Engineers		Self-Declaration with details of NOC
16	DC/DR/Cloud Service Provider Should be providing 24x7x365 shared/dedicated SOC for clients with the help of skilled & certified Engineers		Self-Declaration with details of SOC
17	DC/DR/Cloud Service Provider should be having 24x7x365 dedicated Support Center /Help desk for Incident/Problem management		Self-Declaration with details of Helpdesk

.....

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 4B: Technical Solution Requirements of HCI Solution

S.NO	Item Description	Complied (Yes /No)
1	The solution should provide hyper converged software that allows delivery of enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated component such as SAN Switches & HBAs.	
2	Proposed solution should support the hypervisors listed as a leader in latest Gartner's Magic Quadrant for Virtualization Infrastructure. The solution components quoted including HCI system, hypervisor, server, network switch should be listed as a leader in Gartner's Magic Quadrant for Hyper-converged infrastructure, Hypervisor, modular servers and Data Center Networking respectively	
3	Proposed HCI solution should be 100% software defined without dependency on any proprietary hardware device for deduplication and compression	
4	Proposed solution should support industry leading hypervisor environment viz.Hyper-v, Vmware etc.	
5	The HCI solution should support both hybrid and All-Flash nodes options for future scalability	
6	The proposed HCI solution should be a factory shipped engineered & integrated appliance. All the components of HCI such as compute nodes, hypervisor OS, storage disks, management software should be factory installed and shipped ready for fast deployment.	
7	The HCI solution should support scaling hyperconverged node (compute + storage), compute-only, storage-only (HDDs) independent of each other under a single cluster.	
8	The Solution should support compute only nodes. To add virtual compute capacity to the cluster which can access storage from converged nodes, without incurring any HCI software license cost	
9	The proposed HCI solution should be proposed with N+1 design. The minimum CPU Cores, Memory and storage should be available in the event of any one node failure.	
10	Proposed HCI vendor should have India presence of 10 + years	
11	The proposed HCI solution should support scalability up to 32 nodes in a single cluster. Each server node should have dedicated redundant hot swap power supplies & cooling fans.	
12	The solution should comprise of 10 nodes. Each node should be quoted with min. 2x Intel Xeon Scalable CPUs with 2.4 Ghz, 24c per CPU, populated with 384 GB memory.	

13	The HCI solution should be configured with minimum of 200 TB usable storage capacity excluding cache capacity. The capacity to be configured with minimum data protection of 2 mirror copy of data or higher. The capacity should be absolute capacity without considering any data efficiency techniques as Data Deduplication, compression, erasure coding Any other capacity required for meta data, host maintenance mode, component rebuilds etc. should be factored over and above the capacity.	
14	Solution should support rest API for third party integration and customized workflow for automation using rest API	
15	Min. 4 - 8* 25Gbps network ports per server node.	
16	The hyper-converged system shall include min. 2 Quantities of unified network switches, each with 40 ports per switch with redundant power supplies and cooling fans. The switches should be provided with sufficient 25Gbps for downlink ports and minimum 2*40/100Gb, 6* 25Gps Ethernet ports for uplink connectivity. All required SFPs licenses should be provided.	
17	The network switches included with the HCI solution should be able to connect to existing storage fabric over FC, NFS, ISCSI, m SMB protocols. The vendor should provide the required network switches to support these storage protocols. If any connectivity is not supported additional 2 switches to be provided to support the connectivity	
18	The network switch should support QoS to streamline HCI network traffic to improve traffic filtering, segmentation and performance.	
19	The solution should have multiple vSwitches for network traffic segregation. Various network traffics such as management, storage, virtual machine, vMotion etc. in the HCI should be segregated on to independent virtual switch for improved traffic management and scaling. The procedure must be fully automated in the HCI installation. Any license required should be provided on day 1.	
20	The solution should support Single click non-disruptive rolling upgrades of HCI software and system firmware.	
21	The HCI storage should be a scale-out distributed storage.	
22	The HCI software should pool all HDDs from all the nodes in the cluster to present a single storage resource pool to all server nodes in the cluster. There should not be any dependence on data locality on read, write operations (in production no data locality will be enabled)	
23	The HCI software should pool all SSDs from all the nodes in the cluster to present a single storage cache pool across the HCI nodes.	
24	The HCI solution should support scaling storage capacity and performance linearly by addition of nodes. VMs on existing nodes should get the storage performance & capacity that was scaled by the addition of new HCI nodes.	

25	The HCI solution should be able to present cluster wide storage performance to any single large Virtual machine.	
26	Present scale-out storage to compute only nodes for Seamless failover of compute-only nodes for a fully high available design of HCI	
27	The HCI solution should support connecting to external 3rd party SAN (FC, ISCSI) and NAS (CIFS, NFS) storage into the HCI cluster for capacity expansion and ease of migration from existing environment to HCI	
28	The HCI solution should support various data replication methods 2 mirror data copies, 3 mirror data copies for data protection. Any software license required to enable RF=2 & RF=3 should be quoted from day 1	
29	The HCI solution should support Inline Deduplication across all storage tiers.	
30	The HCI solution should support for 2 nodes failure in entire solution	
31	The Solution should support Instant space optimized point-in-time Snapshots. Should allow for taking snapshots of individual Virtual Machines to be able to revert back to an older state, if required. Any additional software and license should be provided on day 1.	
32	The Solution should allow for taking clones of individual Virtual Machines for faster provisioning. Any additional software or license required should be provided on day 1.	
33	The HCI storage should have integrated wizard to schedule snapshot for hourly/weekly/monthly snapshot policies. Any additional software or license should be provided on day 1.	
34	The HCI storage should have integrated wizard for batch clones of virtual machines and customization. Any additional software or license should be provided on day 1.	
35	The solution should automatically rebalance data to maintain balanced utilization of storage across the HCI nodes. When storage capacity is scaled up or scaled out, the HCI modes must automatically redistribute data equally across all nodes equally without migrating VMs.	
36	The HCI solution quoted should have native replication capability independent on Hypervisor	
37	Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security	
38	Virtualization software should support live Virtual Machine migration with enhanced CPU compatibility and without the need for shared storage option.	
39	Virtualization software should have the ability to live migrate VM files from one storage array to another without any VM downtime. Support this migration from one storage protocol to another (ex. FC, iSCSI, DAS)	

40	Virtualization software should allow for hot addition of vCPU, memory, disk without any downtime.	
41	The CVM sizing should be done considering expansion to full 64 Nodes and all features of HCI highest license software offered enabled. Document for the same to be attached.	
42	The proposed HCI solution with its Hypervisor should support all leading OS including Microsoft & Red Hat. Documents of support from respective OS OEM should be attached.	
43	Virtualization software shall have High Availability capabilities for the virtual machines in the sense if 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. This high availability feature should also be extended to and aware of the applications running inside of the virtual machines.	
44	Virtualization software should have the provision to provide zero downtime, zero 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.	
45	Virtualization software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
46	The solution should provide specific real-time actions that ensure workloads get the resources they need when they need for placement, scaling and capacity decisions. The solution should give options of recommend (view only), manual (select and apply) or automated (executed in real time)	
47	The solution should model what-if scenarios based on the real-time environment to accurately forecast capacity needs	
48	The solution should Track, report, and view trends for compute, storage and database metrics like CPU, memory, IOPs, latency, and Database Transaction etc.	
49	The solution should be able to monitor entire inventory connecting to the virtualization solution, Network switches, 3rd party storage, blade servers etc.	
50	Hypervisor should have inbuilt Distributed Switch to centralize network provisioning, administration and monitoring using data center-wide network aggregation, should provide Network QoS to define priority access to network resources.	

51	the virtualization software should have agentless 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.	
52	Virtualization manager should be highly available with out of box HA without any dependency on clustering software. Virtualization manager should have the capability to monitor other same platform virtualized workloads in the data center	
53	Both Hypervisor and HCI Software license Edition should be latest	
54	The proposed solution should include enterprise grade supported lightweight container management platform for production grade environments, powered by Kubernetes to reduces the complexity of configuring, deploying, securing, scaling, and managing containers.	
55	The solution should provide immutable infrastructure (container as a service) with unified full stack management of host OS, K8s, wizard driven GUI for robust, repeatable user experience. The solution should be integrated & provided with deployment of add-ons (Prometheus, registry, IP mgmt. without external DHCP etc. for ease of deployment & management)	
56	The Proposed container solution should provide and deploy most up-to-date, stable and enterprise ready Kubernetes release with relevant tools and it should allow workloads to be portable between environments.	
57	The Proposed solution should be deployed with container orchestration solution as Kubernetes cluster deployment service. It should include tasks to increase and decrease worker nodes in existing K8s cluster and provision to update and upgrades Kubernetes, cluster version without taking application downtime.	
58	The container orchestration solution should support node pools to provide custom node pools (machine sizes can be different between pools High CPU, GPU, high memory etc.) for better resource management with node resources mapped to add needs as per the application	
59	The solution should provide actionable decisions of container scaling to intelligently scale cluster to provision & suspend nodes based on application resource demands. It should use AI engine to continuously monitor resources and execute action to maintain service performance & availability by identifying which pods could move to which nodes to manage fluctuating demands.	
60	The solution should provide a solution of scaling the clusters by adding or removing worker nodes based on demand by using an autonomous AI/ML engine to provide right actions for every layer of the stack:- sizing:- how to right size the containers (CPU, Mem, N/W utilizations), Placement:- when to reschedule pods to which nodes, auto-scaling:- when to scale in & scale out	

61	The solution should provide for cluster scaling to scale an existing cluster horizontally by adding worker nodes and vertically by changing the size of the nodes/VMs	
62	The solution should provide a provision to create cluster based on requirement and in single click.	
63	The proposed solution should be setup multiple Kubernetes clusters for different environments i.e. Production /Dev/Test as per the requirement	
64	The Solution should provide and must have Deploy OCI compliant enterprise class registry server that stores and distributes container images with vulnerability scanner as part of registry service	
65	The solution should provide and Deploy policy-based image replication between multiple registry instances with auto-retry on errors, offering support for load balancing, high availability, multi-datacenter, hybrid, and multi-cloud scenarios.	
66	Role-based Access Control (RBAC) through built-in static roles, namely the Administrator and User roles enabling to define the provider profile on which clusters can be created	
67	The proposed solution should Integrate with enterprise LDAP/AD systems for user authentication and management' It can also import an LDAP/AD group to registry server and assign project roles to it'	
68	The proposed solution should have GUI with integrated monitoring with Prometheus, Grafana to continuously monitor the health of the cluster deployment to improve the probability of early detection of failures and avoid any significant impact from a cluster failure., log analytics with ELK bundled as part of the platform with security releases & lifecycle management	
69	The Container solution should support management of Helm charts isolated by projects and controlled by RBAC.	
70	The proposed solutions should be able to deploy storage policies to capture storage requirements, such as performance and availability, for persistent volumes. These policies determine how the container volume storage objects are provisioned and allocated within the datastore to guarantee the requested Quality of Service.	
71	Solution to prevent issues by implementing proactive monitoring of the health of all nodes and this should ensure desired responsiveness of the application services by recreating failed / unresponsive nodes.	
72	"The Solution Should Provide and Deploy overlay-based network, advance network services at Layer 2 to 7, Load Balancers (IA and L7), firewall in addition to switching and routing (North-South and East-West) and multi-site networking Layer 2 extension)"	
73	The solution should provide layered security with hardening features (TLS, ECDSA/ED25119, Kubernetes dashboard authorization, protection certification manager, pod security policies etc.	

74	Role-based Access Control (RBAC) through built-in static roles, namely the Administrator and User roles enabling to define the provider profile on which clusters can be created	
75	The solution should be quoted should not restrict to provision containers on all 10N, requisite licenses to be provided for entire cluster capacity (Any license required for container management solution should be quoted over and above),). All the required software/licenses must be included with enterprise class highest tier available with the OEM	
76	The solution should provide single management pane for multi DC management - managing all Data Center site resources from single console.	
77	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network (LAN & SAN), storage, load balancer, firewall other custom services through a unified multi-tenant IT service catalog	
78	The Solution should be multi-tenant and be able to manage roles in a multi-DC, multi-user environment. Users/Tenants should be able to configure their own cloud credentials	
79	The self-service portal should include catalog of services that are provided to the users for consuming the data center resources. The services should include but not limited to,	
80	Provision VM's (Windows/Linux) Application specific infrastructure (Server, Storage, LAN Fabric) Provision bare metal server servers & the users should be able to monitor & create reports for their provisioned infrastructure	
	The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific IT resources, while ensuring compliance with business policies	
81	The proposed solution should monitor organizational usage, trends and capacity, monitor across the infrastructure stack on a continuous basis to improve capacity planning, utilization & management. The solution should show virtual machine (VM) utilization across all your data centers, identify underutilized, overutilized resources	
82	The solution should provide unified dashboards, reports which reduce troubleshooting and performance bottlenecks. It should provide set of compute policies (vCPUs, CPU, Memory reservations, CPU, Memory limit) & provide with resizing options (vCPUS, no: of cores to be configured per socket for a VM etc.)	
83	The solution should include orchestration workflows and tasks that enable you to automate common VM provisioning and proposed hyperconverged solution management tasks	

84	The solution should include out of the box workflows for common tasks like create data stores, ready clones, port groups, edit, delete datastores, replication of VM's hosted on Hyperconverged solution	
85	The solution should have pre-built task libraries for Day 0 automation of infrastructure (SDN, Network, Storage, Hyperconverged, Server, Load balancer, firewall etc.)	
86	The solution should provide automated hardware configuration and Operating System deployment to multiple servers	
87	The solution should have the ability to orchestrate third-party physical & virtual Load balancers, firewalls	
88	The solution should provide native reporting capability & should also provide ability to customize reports and exporting them to multiple formats	
89	The solution shall integrate with Active Directory (AD) to allow importing existing users and groups in addition to creation of local users in the user portal.	
90	The solution shall allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a group of virtual machines to use.	
91	The solution should be able to monitor & manage physical servers from leading server platforms. It should be able to discover & monitor server configurations, manage server lifecycle, perform server use trending & capacity analysis	
92	The Solution Should provide Hardware compatibility matrix for the proposed hardware	
93	The solution should include integration with SDN solutions. It should also include native capabilities to discover & monitor physical network elements, provision VLAN's/VXLAN's across multiple switches, configure SAN Fabric & implement dynamic network topologies.	
94	The solution should have Automated call home capability in the event of critical server failure or thresholds that are crossed which could impact server performance or customer SLA.	
95	The solution should be capable to monitor & manage storage solutions (NAS, SAN) from leading storage vendors. It should be able to provision & map volumes, create, map, expand LUN's, perform SAN zone management & implement storage best practices & recommendation.	
96	The solution shall support granular role-based access control and entitlements of infrastructure services to consumers with continuous monitoring for real-time infrastructure consumption to improve capacity planning and management	
97	Dashboards must be available to allow to control the behavior and consumption of the services	

98	The solution should have ability to accurately forecast future hardware requirements (Storage and Compute) by taking into account the relationship between sizing, placement and capacity across all infrastructure	
99	The solution should provide real Time Visibility and alerting of compliance violations and provide actionable to resolve compliance risks	
100	The solution should support virtual resource management for multiple leading hypervisors (VMware, Hyper-V, RedHat etc.) to access information about the managed VM's, Hosts, datastores and execute commands such as provisioning, resizing or reconfiguring entities sin the environment. can perform system monitoring, report on wasted storage, recommend actions, execute moves for VMs and VM storage, and execute VM reconfiguration (change CPU count, memory, etc.).	
101	The solution should be aware of license compliance, business continuity (DR/HA) at all times. It should provide Real time decisions to prevent or minimize any compliance risks.	
102	The solution should consider all dimensions of application workload demand including storage, network and applications in addition to CPU and memory and applies in decision making	
103	The solution shall support provisioning across multi-vendor physical x86 systems, multi-hypervisor (eg: VMware ESX 6.7 or higher, Microsoft Hyper-V 2016, System Center 2016 or higher and Red Hat hypervisors) virtual environments.	
104	The solution should provide vertical and horizontal scaling of workloads and automate provisioning of infrastructure resources.	

.....

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 4C: Technical Solution Requirements of Data Centre Security & Network Solution

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

Sr No	Specifications	Compliance (Y/N)
1 . Hardware Architecture		
1.1	The proposed appliance must have minimum 4 x 1G copper RJ45 ports from day one. The appliance must have minimum 4 x 1G SFP from day one. The Appliance must have minimum 4 x 10G SFP + slot from day one so ECGC can add SFP+ as and when required. HA, Sync & Management port must be provided separately.	
1.2	The proposed appliance must have - 1 x 1G port for out of band management - 2 x 1G port for HA connectivity These ports must be in addition to production ports mentioned earlier.	
1.3	The proposed solution must have minimum 240GB SSD drive for storing operating system image, system files, system logs & network traffic logs.	
1.4	The Appliance must have minimum 16 GB RAM from day one.	
1.5	The appliance must have 2 x redundant power supplies from day one.	
1.6	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).	
1.7	The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.	
2 . Performance Requirement		
2.1	The proposed firewall must provide NGFW functionality from day one. All required license must be provided from day one.	
2.2	The proposed firewall must provide minimum 2 Gbps of	

	throughput with encryption (when Firewall & App Control feature enabled) with Real world HTTP traffic of 64K transaction size and not Video/JPEG based traffic (enterprise testing condition). OEM to provide publicly available document mentioning throughput with transaction size, traffic mix & feature enabled including App-ID, User-ID, Content-ID, DoS/DDoS & Logging enabled	
2.3	The proposed firewall must provide minimum 1 Gbps of threat prevention throughput with Real world HTTP traffic of 64K transaction size and not Video/JPEG based traffic (enterprise testing condition). The throughput must remain 1 Gbps even after enabling NGFW + IPS + AntiVirus + Anti Spyware + Anti Bot + DoS/DDOS + All signature enabled + Logging enabled + Bidirectional inspection + File Blocking. OEM to provide publicly available document mentioning throughput with transaction size, traffic mix.	
2.4	The proposed appliance must support minimum 190,000 concurrent sessions with Real world HTTP applications and not based on UDP / Lab environment / ideal testing environment.	
2.5	The proposed firewall must support minimum 12,000 new session per second with real world HTTP application and not based on UDP / Lab environment / Ideal testing environment	
2.6	The proposed firewall must support SSL decryption. It must support minimum 18000 concurrent decrypted session. OEM has to provide public document as reference	
2.7	The proposed vendor must have "Recommended" rating in NSS LABS test with min 99% Evasion block capability and min 97.5% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall Test Report.	
3 . Firewall Features		
3.1	The proposed firewall must be a L7 - Application aware - NGFW from day one.	
3.2	It must allow to create security policies based on L7 parameters such as Application, Users, File Type etc in addition to IP & Port numbers.	
3.3	While creating application based policy the firewall must auto select all default port numbers without need of admin to mention it separately. Example - while allowing Active Directory as an application, firewall must auto include all relevant port numbers used for AD communications such as 135, 138, 139, 389, 445 etc	
3.4	Preferred to have informational or warning message to admin about dependent application to be included in policy to avoid application misbehaviour	
3.5	The firewall must allow user identification by integrating	

	with AD, WIFI, NAC etc solutions.	
3.6	The firewall must able to identify users behind Proxy server by reading information in XFF header and perform User-ID mapping. The firewall must strip XFF information before forwarding traffic to internet for privacy reason.	
3.7	The Firewall must support Active - Passive & Active - Active deployment option with IPV4 & IPV6 with seamless failover between HA pairs. The Firewall must support Multi device clustering as well.	
3.8	The firewall must able to identify end user ip addresses even if user traffic is coming via content delivery network such as Akamai by reading information in XFF header. The Firewall must allow Bank to create security policy based on IP Address information in XFF. Example - If SSL want to block bad IP addresses of China, Firewall must able to detect these IP Addresses even if Chinese are coming via Akamai CDN with USA / Europe as source IP and block such traffic instantly.	
3.90	The firewall must allow SSL to create security policy for API Based payment applications & next generation Cloud Native applications where IP Address & URL keeps on changing and its practically impossible to keep a track and update firewall policies. The Firewall must have ability to allow customer to create security policy to allow such API based payment application without need to worry about IP address. Example security policy for googleapis.com etc	
3.10	The firewall must have ability to track application response to ensure easy troubleshooting in case if application is misbehaving. Example ideal response expected from web server is HTTP 200 OK, instead if web server is sending HTTP 404, Firewall must able to track and flag it to admin.	
3.11	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 limit for the capture.	
3.12	The firewall must support FQDN instead of IP address for static route next hop, policy based forwarding next hop.	
3.13	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	
3.14	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, Bit torrent, YouTube, azureus)	
	-by static or dynamic application groups (such as Instant Messaging or P2P groups)	
	-by port and services	
3.15	The NGFW must provide immediate visibility into applications bypassing traditional security policy & running on non-standard ports in the ECGC environment. The Firewall must able to provide comprehensive report with Source/Destination IP, Application name (real application name & not protocol), source & destination Zone, data transfer amount & file name transfer. So ECGC team can preventive action accordingly. Example DNS application running on any other port then 53.	
3.16	The NGFW must be able to acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing	
3.17	The NGFW must offer full and unfettered open API Support without a paywall (subscription) to access Dev toolkit, Tools and Scripts and samples.	
4 . Security Features		
4.1	The firewall must support comprehensive threat prevention security features including IPS, Antivirus, Anti Spyware, Anti Bot, DoS/DDOS etc from day one.	
4.2	The proposed firewall must have integrated Intrusion Prevention Systems - IPS with ability to prevent ECGCs critical trading applications and digital asset against minimum 15,000 + vulnerability exploit attempts. The firewall must detect & prevent minimum 12,000 + CVE exploit attempts to safeguard ECGC environment. OEM to provide full list of IPS signatures along with CVE numbers.	
4.3	The proposed firewall must support attack recognition for IPv6 traffic the same way it does for IPv4	
4.4	The proposed solution must support different actions in the policy such as deny, drop, reset client/server	
4.5	The proposed solution must have functionality of Geo Protection to Block the traffic country wise per policy and per applications as per customer requirement and shouldn't be a global parameter	

4.6	The proposed solution must have an option to create custom signatures. It should also support importing of rules automatically from other open source solutions like, SNORT or Suricata etc.	
4.7	The Firewall must support ability to decrypt & inspect TLS 1.3 traffic.	
4.8	The proposed firewall must support ingesting 3rd party IOCs such as IP Addresses, Domain Names & URLs from different sources including existing security solution such as FireEye, Trend Micro & Open source threat intel such as Talos, Spamhouse etc.	
4.9	The NGFW must support QoS marking and reclassification based on source/destination IP, port, protocol, user, applications, security zone etc.	
4.10	The proposed vendor must have "Recommended" rating with min 99% Evasion proof capability and min 97.5% Security Effectiveness as per 2019 NSS Labs Next Generation Firewall comparative Test Report.	
4.11	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	
4.12	All the proposed threat prevention functions like IPS/vulnerability protection, Antivirus, C&C protection etc should work in isolated air gapped environment without any need to connect with Internet.	
4.13	Firewall should have specific DNS Security Signature Categories of domains based on the risk that these domains pose to ECGC. ECGC should be able to block DNS based attacks for include C2 (encompasses DGA and DNS tunnelling), malware, DDNS, newly registered domains, and phishing	
4.14	Should have simple policy formation for dynamic action to block domain generation algorithms or sinkhole DNS queries.	
4.15	The NGFW must have ability to detect credential theft attempts on ECGC employees. In such cases, NGFW must block the traffic & reset the session immediately. NGFW must provide ability to enable / disable it as per ECGC requirement.	
4.16	The NGFW Anti-virus & anti Malware must able to analyse	

	& prevent malicious file, virus, malware, ransomware etc traversing on following protocols: HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP, and SMB.	
4.17	The NGFW must be able to support decryption of the following protocols: SSL, SSH	
5 . Management		
5.1	The firewall must support on device management for config changes.	
5.2	The firewall must have CLI, SSH & HTTPS based on device management	
5.3	The firewall must have full-fledged on device management allowing all possible config to be performed directly on the firewall.	
5.4	The firewall must have comprehensive logging, log analyser, log correlation, search, filter, unified logs available directly on firewall or on a separate logging server	
5.5	The solution must provide Executive Dashboard - Highlight Customizable Dashboard to provide quick insight to Applications / Users / Content / Files / Threat / Top Country / Top Rule Usage	
5.6	It must provide immediate visibility to all applications including internet + enterprise + generic + unknown applications. The report must highlight applications running on non-traditional ports and by- passing L3/L4 security rules so ECGC can take immediate action. Example SSH is running on 443, SSL running on 80 etc. NGFW must provide report including source IP / User / Destination IP / Hostname / byte transfer / rule allowing non-standard traffic in a GUI and must be exportable in PDF format.	
5.7	OEM / Bidder must propose NGFW with in-built + easy to use + GUI Based + automated + non disruptive + zero touch policy migration from existing L3/L4 to L7 - Application Layer within a month of NGFW deployment. OEM must ensure that there is no packet drop + no disruption + false positive post migration.	
5.8	Proposed NGFW solution should have separate control and data plane with their own resources like CPU, Memory & Storage to ensure continuous & uninterrupted access without any lag or delay to NGFW irrespective load & CPU utilization. In an unplanned & unforeseen event, Security admin must able to login to NGFW, collect logs, make necessary changes and commit changes in to NGFW	

5.9	In order to ensure NGFW is deployed as per industry best practices + OEM best practices + avoid misconfiguration + avoid Human error, ECGC Would like to review the NGFW config on a monthly basis. Bidder / OEM to provide online, GUI based, easy to use tool for best practice assessment. Bidder / OEM to provide comprehensive report highlighting config gap against best practices & provide steps to rectify them. This assessment needs to be conducted on monthly basis and progress (to fill identified gaps) needs to be tracked & presented to ECGC on monthly basis.ECGC must able to generate the report directly by themselves without involving bidder & OEM.	
5.10	Firewall must identify the amount of TLS traffic, non-TLS traffic, decrypted traffic, and non-decrypted TLS traffic, number of ssl sessions in a separate section for better visibility and troubleshooting. Firewall should also show decryption failure (if any) reason data in GUI for troubleshooting	
5.11	The solution must have the native capability to optimize the security rule base and offer steps to create application based rules	
5.12	The proposed solution must allow 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.	
5.13	The NGFW must support the ability to create custom reports directly from the WebGUI of the NGFW	
5.14	Would be advantage when NGFW should support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed or equal features.	
5.15	The NGFW must be able to tag objects to enable dynamic enforcement of policy no matter any changes to IP, area, or direction traffic originates from with no need to recommit policy	
5.16	The NGFW must be able to provide scalable clustering and multi DC clustering.	

(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	
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 and Web application Firewall	
3	The appliance should have minimum 4*40G QSFP+ & 8*10G SFP+	
4	Appliance should support L7 requests per second: 1.8M	
5	Appliance should support L4 connections per second: 800K	
6	Appliance should support L4 HTTP requests per second: 12M	
7	Appliance should support Maximum L4 concurrent connections: 40M	
8	Appliance should support Throughput: 60 Gbps/35 Gbps L4/L7	
9	Appliance should support 20 Gbps bulk SSL encryption	
10	Appliance should support ECC†: 20K TPS (ECDSA P-256) / RSA: 35K TPS (2K keys)	
11	Appliance should support Virtualization upto 8 instances	
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	The appliance should support global server load balancing algorithms including - Weighted round robin, Weighted Least Connections, Administrative Priority, Geography, Proximity	
21	GSLB solution should able to evaluate round trip time (RTT) and hop count for dynamic proximity calculations.	
22	The Solution should have Dedicated SSL Chipset for SSL Offloading which ensures SSL offloading should be done by dedicated hardware instead of shared CPU. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.	
23	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation	
24	The appliance should support Certificate format as "*.PEM", "*.PFX", "*.CER"	
25	Solution shall provide advance health checks based on HTTP, HTTPS and TCP/UDP protocols	
26	Should support advance ACL's to protect against network-based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.	
27	The proposed Load balancer should support ICAP integration with AV and other third-party solutions.	
28	The proposed solution must support TCP multiplexing, TCP optimization and dynamic Service chaining for SSL Offload.	
29	It should natively support Geolocation data base without any additional licenses and provide regular updates on OEM's website	
30	System should support Standard HTTP, Explicit HTTP, and Transparent HTTP profiles natively without need of scripting	
31	Load balancer should support NodeJS which can be used with native scripting language to give better control on the network traffic.	
32	Load balancer should support creation of Virtual servers which can be categorically offloaded to hardware chipsets. The level of offload to chipset function should also be customizable	
33	Load Balancer should have native MQTT, SIP, Diameter routing agent for optimum control on traffic.	
Web Application Firewall		
34	The WAF solution should be in the Gartner's Leaders	

	Magic Quadrant for "Web Application Firewall" for any one year in the last five published reports.	
35	The Solution should meet PCI DSS Compliance as per PCI DSS requirement and should provide reports for PCI DSS compliance.	
36	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. (The bidder should describe how each of the OWASP Top 10 vulnerability is addressed by the solution).	
37	The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	
38	The Proposed WAF Solution must support deployment as inline proxy, one arm mode or similar.	
39	When deployed as a proxy (either a transparent proxy or a reverse proxy), the Web application firewall should be able to digitally sign cookies, encrypt cookies, and to rewrite URLs.	
40	The Proposed WAF Solution should support both a Positive Security Model and a Negative Security Model and also should provide regular update for CVE signatures.	
41	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage. Should provide facility to configure time for staging of policy and policy should move to blocking once staging time is over.	
42	The solution must be able to block transactions with content matching for known attack signatures while allowing everything else.	
43	The solution must support and integrate with the following web application vulnerability assessment tools (Web application scanners) at minimum to virtually patch web application vulnerabilities: Whitehat Sentinel, IBM Appscan, Rapid7 and QualysGuard, for rapid virtual patching.	
44	Should be able to import Vulnerability scanner report from Whitehat Sentinel, IBM Appscan, HP Webinspect, Rapid7 and QualysGuard and fixed those vulnerabilities within the waf using xml file.	
45	The solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode.	
46	The solution must support user tracking using both form-based and certificate-based user authentication. Solution	

	should support API security including support for uploading swagger file.	
47	The solution must be able to validate encoded data in the HTTP traffic	
48	The solution must be able to identify Web Socket connections and provide security for WebSocket including exploid against Server abuse, login enforcement, XSS and SQL injection.	
49	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection\learning mode.	
50	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.	
51	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	
52	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	
53	The Proposed WAF Solution should have capability to mitigate, learn and adapt to unique application layer user interaction patterns to enable dynamic defenses based on changing conditions	
54	The Proposed WAF Solution should have Correlated Attack Validation capability or Correlation features which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.	
55	The Proposed WAF Solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.	
56	The Proposed WAF Solution Should support ICAP integration with other security devices for file scanning.	
57	The proposed WAF Solution should be configured with real-time threat intelligence on known malicious sources, such as:	
	Malicious IP Addresses: Sources that have repeatedly attacked other websites	
	Anonymous Proxies: Proxy servers used by attackers to hide their true location	
	TOR Networks: Hackers who are using The Onion Router (TOR) to disguise the source of attack	
	IP Geolocation: Geographic location where attacks are coming from and block access	

	Phishing URLs: fraudulent sites (URLs) that are used in phishing attacks.	
58	The Proposed WAF Solution should accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, etc. It should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating using JavaScript, Image and Sound CAPTCHA challenges. This information should drive WAF policy enforcement decisions, including handling bad and suspected bots. Administrators should also receive an alert (e.g. for monitoring purposes), or have capability to block the bot.	
59	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behavior analysis, reverse DNS lookup	
60	The Web Application Firewall should have "Anti-Automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.	
61	The Proposed WAF Solution should have Threat Intelligence to Identify New Attack Vectors. Community Defense feature gather suspicious Web requests, validate that requests are attacks, and transform identified attacks into signatures.	
62	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioral analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack.	
63	Solution should support Behavioral L7 DDoS mitigation to detect attacks without human intervention.	
64	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	
65	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	
66	The Proposed WAF Solution must have an option to have "Comment Spam IP Feed" to Block IPs to reduce spam messages in forums and user boards of customer web applications.	
67	The Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client-side malwares	
68	The Proposed WAF Solution should protect API based communication between client & servers using all the relevant WAF signatures.	
69	Should provide encryption for user input fields to protect from browser based malwares stealing users credentials	

70	Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	
71	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.	
72	The solution must allow administrators to add and modify signatures.	
73	Proposed Solution should have ability of HTTP response logging.	
74	Solution should offer protection for FTP and SMTP protocols.	
75	Solution should support user-written scripts, that provide flexibility to control application flows.	
76	Proposed Solution Attack log entry should have action to accept further request like this in policy or reject such an attack in future.	
77	Proposed Solution should have ability to differentiate DoS mitigation action based on Attacker Source IP, device fingerprint, URL or Geolocation.	
78	Proposed Solution should have ability dynamically generate signatures for L7 DoS attacks. These signatures should be exportable for use on 3rd party systems.	
79	Proposed solution should be able to track unused elements in the policy and suggest to remove them after a specified period of time	
80	Proposed Solution should have ability to automatically detect software technology used on backend side to define signature sets required for defined Proposed Solution policy.	
81	Proposed Solution should have ability to configure way to analyze request payload based on custom rules for each URL entry configured in the security policy	
82	Proposed Solution should be able to track application changes over time and adjust config elements and rules based on that data.	
83	The solution must support regular expressions for the following purposes: Signatures definition, Sensitive data definition, Parameter type definition, Host names and URL prefixes definition, Fine tuning of parameters that are dynamically learnt from the web application profile.	
84	The WAF instance should have option to enable x-forwarder option per service to log actual client IP in webserver logs even deployed in Reverse Proxy mode.	

85	Separate policies should be applied for different applications configured on the same WAF	
86	The solution should have pre-built templates for well-known applications eg., ActiveSync, SAP, Oracle Applications/Portal. Solution should have the ability to build a base policy and inherit child policies from the same. Inheritance should support restricting modifications to the base policy settings	
87	All web facing applications are to be integrated to WAF without any limitation on the number of applications. Solution should support the deployment modes based on application needs	
88	Should support Integrated Web Application Load balancing that helps to reduce latency and gives singular window of management. WAF & Load balancer should be on the Device	
89	Proposed solution should be able to integrate with external SSL visibility solution	
90	The solution should also support sending of logs in CEF (Common Event Format) standard	
91	Proposed solution should support multiple administration domains (or partitions) to configure and administer the system. This would include support for using remote authentication servers (e.g. LDAP, Windows AD, RADIUS and TACACS+) to store system user accounts.	
92	Proposed solution should provide account creation with access level that can • Provides User roles that can be assigned such as Administrator, Resource Administrator, User Manager, Manager, Application Editor, Application Security Policy Editor, Operator, or Guest. It can be no access for user account to system resources Provide administrative partition(similar) where it limits user access to certain device objects which include entities that user accounts can manage and place in administrative partition.	
93	Proposed Solution should have Role-based management with user authentication. There should be web application security administrator whom has access to web security policy objects in web profile, modify web profiles but cannot create or delete those profiles, and web application security editor(similar) whom configure or view most parts of the web security policy object in specific controlled partition holding the policy and profile objects.	
94	Organization should be able to deploy or remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.	
95	Should be able to view and compare policies.	

96	Native support for Geolocation data base without need of additional licenses	
97	The WAF should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc.	
98	Transactions with content matching known attack signatures and heuristics based should be blocked.	
99	The Web application firewall should allow signatures to be modified or added by the administrator.	
100	Visibility to Application Security (System should support dashboard view (either via GUI or Centralised Management Console) for Mitigated attacks, Prominent attacks etc.)	
101	IP Reputation Database Support (System should identify the IP address that is sending unwanted requests). It should be able to block scale DDoS, DoS, or anomalous syn flood attacks from known infected sources. Database should get updated automatically once within 30 min or so.	
High Availability		
102	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR	
103	Should support transparent failover between 2 devices, the failover should be transparent to other networking devices with SSL session mirroring	
104	Should support network-based failover for session mirroring, connection mirroring and heartbeat check	
105	Device level HA should support automatic and manual synchronization of configuration from primary device to secondary device	
Centralized Management & Analytics		
106	Centralized Management Software should provide a unified point of control for the Device (including modules for SLB, WAF and GSLB) and should be able to push centralized software updates. This Software should be supplied as a separate software other than WAF/SLB devices	
107	Should manage policies, licenses, SSL certificates, images, and configurations for all the appliances	
108	Should have predefined roles/permissions configurations to manage who can see application dashboards, and edit and deploy services and policies for application delivery and security. Roles can be associated with local users and groups, or users and groups from remote RADIUS or LDAP servers.	
109	Should be able to leverage a declarative model to create, import, and edit AS3 templates to use when deploying application services making it easy to integrate with Netops team automation toolchain	

110	Should provide extensive visibility into the health and performance of applications with dashboards to highlight applications with longest response time, top HTTP transactions, Top connections. It should be able to pinpoint applications that need attention quickly and help to drill down to the root cause of performance per application	
111	Should be able to view and compare policies.	
112	Should be able to monitor Bot Defense with real-time visibility to reflect the amount of automation traffic hitting the applications	
113	Should be able to Enable, manage, and deploy threat campaign mitigations	
114	Device should support config automation using ansible modules without OEM workflow parser. This helps Ansible tower to directly communicate with Device for config automation.	
Monitoring & Logging		
115	Solution must support SNMPv3, Syslog	
116	System must support external authentication including LDAP, TACACS+, RADIUS	
117	Easy-to-use graphical user interface for visualization and top-level management, also the device console or CLI should be easily accessible if needed	
118	Should support SSHv3 and HTTPS access.	
119	Should have ability to upgrade/downgrade device software Images.	
120	Proposed solution should also integrate with SIEM solutions	
Support		
121	The OEM should have a Technical Assistance Center (TAC) which Follow the Sun Model with toll free numbers	
122	The OEM should have Support Centers / Service Center or 24x7x365 TAC Support	
123	The Proposed WAF Solution should be provided with hardware replacement warranty and Ongoing Software Upgrades for all major and minor releases during the completion of project	
124	OEM should have Local Stocking of Spares within the Country to ensure that the SLA is not breached	

(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 / ICSA / EAL4 or more.	
3	Proposed solution should not declared with eol, eos or end of support by OEM.	
Technical Specification		
4	Stateful inspection firewall throughput (multiprotocol) should be min 20 Gbps	
5	Firewall shall support up to 5 million Concurrent connections	
6	Should be able to support 200,000 connections per second	
7	Firewall License proposed must include all required features given in tender.	
8	Should have 8x 1GE RJ-45 interfaces, 4x 1GE SFP, 1xGE Management & 1 Console interfaces with auto sensing capacity and option to expand further.	
9	Should have at least one Management and console port	
10	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), PIM-SM/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	The Proposed firewall Solution should be able to work in High Availability (HA) mode & operate on either Transparent (bridge) mode or NAT/Route mode.	
20	Appliance should support a LCD panel/LED to display alerts and fault information for an administrator to monitor the system	
21	The appliance should have redundant power supply	
22	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		
23	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	
24	OEM should have Local Stocking of Spares within the Country to ensure that the SLA is not breached	
25	OEM of the Proposed Solution Vendor should provide regular updates to geo-location database from their public downloads website	
26	OEM should have a Technical Assistance Center (TAC) which Follow the Sun Model with toll free numbers	
27	The Support should be of production/Enterprise support level. For Highest Priority Calls (P1 – Calls), response to be provided by OEM within 15 minutes. The Expected resolution Time is 4 hours (maximum).	
28	OEM should have Support Centers / Service Center in India	
29	The devices and software support should be provided for 5 years after deployment.	

(4) Technical Specification of L3 Switching

S. No	Item Description	Compliance (Yes/No)
1	The model considered should not be out of support for at least five years from date of purchase. Vendor needs to acknowledge this.	
2	Core Switch should offer Wire-Speed Non-Blocking Switching & Routing Performance at Layer 2 and Layer 3.	
3	Each Core Switch should be configured with twenty-four (24) 1GbE SFP Slots / 10GbE SFP Slots	
4	Core Switch should support Active-Active Dual Core Configuration using Virtual Switching System (VSS) or Virtual Chassis (VC) or equivalent Switch Clustering feature.	
5	Switching Bandwidth: Core Switch should provide Non-Blocking switch fabric capacity of 1.44Tbps or more	
6	Forwarding Capacity: Core Switch should provide wire-speed packet forwarding of 1.07 Bpps or more.	
7	Core Switch should support 4K Active VLANs	
8	Core Switch should support 288K MAC addresses or more.	
9	Core Switch should support IP multicast snooping IGMP v1, v2, v3	
10	Core Switch should support Jumbo Frames (up to 9,216 bytes)	
11	Core Switch should support minimum 64K IPv4 routes or more	
12	Core Switch should support Basic IPv4 and IPv6 Static Routing, ECMP, Host Routes, Virtual Interfaces, Routed Interfaces, Route Only and Routing between directly connected subnets from Day 1.	
13	Core Switch should support the following Dynamic IPv4 & IPv6 Routing protocols and Multicast Routing Protocols from Day 1.	
14	Dynamic IPv4 and IPv6 Routing protocols like RIP v1&v2, RIPng, OSPFv2, OSPFv3, BGP4, BGP4+, Multi-VRF, VRRPv2 & VRRPv3. All licenses to be mentioned clearly.	
15	PIM-SSM, PIM Sparse, PIM Dense, PIM Anycast RP, and PIM passive IPv4 multicast routing.	
16	IPv4 Multicast Non-stop routing (NSR) support for PIM-SM, SSM, and Anycast RP.	
17	PIM-SSM, PIM Sparse, PIM Anycast RP, MSDP	
18	Core Switch should support RADIUS, TACACS/TACACS+ and username/password for Authentication, Authorization and Accounting (AAA) with Local User Accounts and Local User Passwords.	

19	Core Switch should support secure communications to the management interface and system through SSL, Secure Shell (SSHv2), Secure Copy and SNMPv3	
20	Core Switch should support IP Source Guard, DHCP snooping, DHCPv4, DHCPv6 and Dynamic ARP Inspection.	
21	Core Switch should support IPv4 and IPv6 ACLs	
22	Core Switch should support Flexible Authentication with 802.1x Authentication and MAC Authentication.	
23	Core Switch should support manageability using Network Management Software with Web based Graphical User Interface (GUI).	
24	Core Switch should provide Integrated Standard based Command Line Interface (CLI), Telnet, TFTP, HTTP access to switch management/monitoring	
25	Must support automation features to reduce administrative workload. Features include zero touch provisioning (ZTP), operations and event scripts, automatic rollback, and Python scripting.	
26	The switch also offers support for integration with VMware NSX Layer 2 Gateway Services, Puppet, and OpenStack.	
27	Core Switch should support NetFlow or sFlow or equivalent	
28	Core Switch should be provided with 19" Universal 4 post rack mount kit	
29	Core Switch should be loaded with dual hot swappable, redundant load sharing AC power supplies to provide 1:1 power supply.	
30	Core Switch should be loaded with dual hot swappable, redundant fans.	
31	Core Switch should be quoted with TAC Support and Warranty for 5 years with NBD Hardware Replacement.	
32	The Predicted mean time between failures (MTBF) must be at least 150,000 hours	

(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 nos of cables minimum 5m in length per switch for connectivity of HCI nodes and Backup server to 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/HCI 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 HCI Solution & meets all the requirements of HCI	
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 DDI (DNS-DHCP-IPAM) Specification:

	DNS Functionalities	Compliance (Yes/No)
1	The proposed solution must provide dedicated platforms purpose-built hardware/VMs.	
2	The proposed solution can support Authoritative & Recursive DNS functions	
3	The proposed solution can be offered on either hardware appliance or VNF (Virtual Network Function) for different components	
4	The proposed solution must use a purpose-built, hardened operating system. No need for additional hardening or tunning of OS	
5	If the appliance used a linux based system, the proposed solution must garantee the access using linux system accounts is disabled to avoid the explotation of vulnerabilities due the OS libraries	
6	The proposed solution must be deliver in a system that does not require independent maintenance of the operative system, updates and service.	
7	Proposed DNS solution shall be possible to be deployed either physical or VNFs within the same management system.	
8	The proposed solution must assure the lowest possible latency for cached responses through (hardware oe DPDK) cache acceleration.	
9	Proposed DNS solution shall be flexible to integrate with an Orchestration layer and automate deployment with elastic scaling.	
10	The proposed solution should provide Low Latency responses in micro-seconds	
11	The proposed solution must scale up to million responses per second (QPS) to manage rapid increases in DNS queries.	
12	The proposed solution must support fault tolerant caching in case in case of authoritative service downtime.	
13	DNS Recursive support for ECS (edns0 Client Subnet)	
14	Vendor to provide Solid References within Service Providers customers across the region	
15	The solution to handle IPv4 DNS queries (all query types)	
16	The solution to handle IPv6 DNS queries (all query types)	
17	The solution to working in IPv4, IPv6 and IPv4v6 dual stack mode (all query types)	
18	The solution to work as DNS64 (all query types)	
19	Solution must support standards-based DNS services	
20	Management platform must provide safety mechanism to ensure that concurrent administrators do not conflict each others changes at a zone level	
21	Product must support the ability to specify a custom list of root name servers	

22	Product must support the ability to act as an internal root name server	
23	Product must support Anycast for DNS	
24	Product must support Bidirectional Forward detection (BFD) for OSPF and BGP	
25	Product must automate common tasks such as glue A record creation to prevent errors	
26	Product must automate common tasks such as maintaining synchronization between forward and reverse records	
27	Product must support the ability to manage the data hierarchically with over-rides at device/zone/record level	
28	Product must support the ability to centrally manage name server groups which can applied to zones	
29	Product must support adding the following types of DNS records: A, AAAA, MX, CNAME, DNAME, TXT, SRV, PTR	
30	Product must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)	
31	Product must support access control lists (ACLs) for Zone Transfers.	
32	Product must support access control lists (ACLs) for queries.	
33	Product must support access control lists (ACLs) for recursive queries	
34	Product must support BIND's views feature	
35	Product must support the ability to have records shared between views and zones (similar to the BIND $INCLUDE statement)	
36	Product must support the ability to centrally manage, configure and report on compliance with RFC-based and customer-defined hostname checking policies (Strict, Allow Underscore, etc.)	
37	Product must support enforcing configurable restrictions on the format of hostnames to comply with RFCs and internal company policies	
38	Product must support incremental zone transfers	
39	Product must support TSIG for authentication of zone transfers and dynamic updates	
40	Product must support the ability to control DNS logging	
41	Product must provide DNS statistics such as Successes, Failures, Referrals, NXDomain responses, etc	
42	Product must support the ability to view DNS data in different ways (by zone, by server) in order to easily determine which data are served by each server, or to manage zones independently of name server	
43	Product must support the ability to search for a record in any zone	
44	Product must support common tasks such as sorting and filtering DNS records and associated meta-data	
45	Product must support the ability to associate other data with DNS records such as device type, serial number, location, etc.	
46	Product must support the ability to selectively restore any zone(s) that have been deleted, without having to restore other zones	
47	Product must support the ability to delegate administration of zones	

48	Product must support the ability to delegate administration of different resource record (RR) types	
49	Product must support the ability to delegate administration for individual DNS objects	
50	Product must allow for recursive only service.	
51	Product must allow for authoritative only service.	
52	Product must support the ability view DNS syslog messages	
53	Product must support EDNS0	
54	Product must support a recent version of BIND 9, at least 9.3.0	
55	Product must support an advanced forwarder selection algorithm, such as choosing a forwarder according to roundtrip time	
56	Product must support diagnostic capabilities such as DNS query latency monitoring	
57	Products must be available in different sizes for queries per second	
58	Must support DNS Firewall using industry standards RPZ feeds.	
59	Must support vendor supplied and external RPZ feeds.	
60	Vendor must provide and support high quality dynamic malware data feed with frequent updates	
61	Vendor must be capable to integrate with 3rd party feeds via Response Policy Zones (RPZ)	
62	Vendor must have tool that security analysts can use to report on why domains were classified as malicious by the DNSFW/threat feed (Threat Lookup)	
63	Vendor must have reporting tool to summarize and report on locally sourced malicious traffic, e.g. Top malicious domains, Top clients that tried to communicate to malicious domains, etc.	
64	Must be able to balance GTP tunnels across multiple gateways	
65	Must be able to detect GTP availability of gateways and remove broken gateways from the DNS responses.	
66	Must provide the hardest security to withstand volumetric and DNS based attacks	
67	Must avoid operator error at data entry.	
68	Must support role based access control	
69	Must provide an audit trail of all moves adds and changes.	
70	Support for DSCP	
71	Solution must support algorithmic pre-fetching of frequent domains	
72	Solution must support retaining the last cached value for a Resources Record when an authoritative DNS is offline	
73	Must have the capacity to provide high geographic availability by using Anycast	
74	Accepting dynamic DNS updates (DDNS) in real time	
75	Detection and mitigation of DNS security attacks, with the ability to alert via SNMP and / or e-mail	
76	DNSSEC configuration (signing and maintenance of zone signatures) according to NIST-800-81, with automated mechanisms to eliminate manual operations	

77	DDNS updates with GSS-TSIG from Microsoft clients to the DNS server	
78	Zone blocking, which allows a single administrator to modify a zone to thetime	
79	DNS redirection and filtering	
80	Host name templates, which allow the rules of those names to be applied	
81	RFC's for DNS: 805, 811, 819, 881, 882, 883, 897, 920, 921, 073, 974, 1032, 1034, 1035, 1101, 1122, 1123, 1178, 1348, 1386, 1464, 1535, 1536, 1537, 1591, 1611, 1612, 1637, 1664, 1713, 1794, 1811, 1816, 1912, 1956, 1982, 1995, 1996, 2010, 2052, 2053, 2136, 2142, 2168, 2181, 2182, 2219, 2240, 2308, 2317, 2352, 2537, 2606, 2671, 2782, 2845, 2915, 3596, 3645, 3768, 4033, 4034, 4035, 4641, 4956, 4986, 5155, 5702, 5936, 6147.	
DNS High Availability		
82	The solution must provide high availability at different levels:	
83	o Appliance high availability, e.g. cluster or HA pair	
84	o Appliance failover must be based on standardized protocols and must be executed without any administrator interference. Failover times shall be below 5 seconds in failure case and below one second in operator initiated failover case	
85	The solution must provide Anycast service with Bidirectional Forwarding Detection (BFD) protocol for fast convergence Anycast embeded with DNS engine	
86	The solution must provide DNS Anycast convergence time with less than 1 second with BFD.	
87	The solution must provide DNS engine integration with BFD protocol to detect DNS resolution failures and deactivation routing advertisement for Anycast and BFD protocols	
88	The solutions must provide DNS Anycast with protocols BGP and OSPF	
89	The system must support fault tolerant caching in case in case of authoritative service downtime.	
90	All networking configurations must be done from the centralized console and be audited	
DNS Security		
91	The proposed solution must support several layers of security.	
92	The solution must provide signature based security measures.	
93	The solution must provide reputational security measures.	
94	The solution must provide behavioral security measures.	
95	The minimum layers of security are:	
96	o Advanced DNS Protection: Defense based on Signature and Volumetric DdoS	
97	o DNS Firewall	
98	o DNS Analytics	
99	o Value Added Services	
100	Each security layer must be switched on / off and tuned independently.	

101	The proposed solution must provide security protection covering full IP attack surface, including IP stack protocols (ICMP, TCP/UDP, BGP, OSPF) , Operating System and DNS protocol	
102	The security protection must be managed with centralize management, with policy distribution for all IP stack layers	
Advanced DNS Protection		
103	The proposed solution must defend itself against volumetric attacks. Defense must not only cover the DNS protocol but also all other supporting protocols needed for DNS service delivery like NTP, BGP, OSPF, BFD, UDP, TCP, SNMP etc.	
104	The proposed solution has to provide updates to the security protection rules.	
105	The operator must be able to customize security rules.	
106	The proposed solution MUST support DNS Security features below:	
107	DOS	
108	DNS Exploits OS and application vulnerabilities	
109	Semantic attacks	
110	Reconnaissance	
111	DNS Amplification and Reflection Attacks	
112	Cache poisoning	
113	TCP SYN Flood Attacks	
114	UDP Flood Attack	
115	OSPF, BGP, BFD, NTP attacks	
116	Spoofed Source Address/LAND Attack	
117	Protocol anomalies	
118	NXDOMAIN Attack	
119	SERVFAIL Attack:	
120	DNS hijacking	
121	DNS Tunneling	
122	DNS Malwares	
123	Random sub-domain (slow drip attacks), Domain look-up attacks	
124	Phantom domain attacks	
DNS Firewall		
125	You must implement a mechanism to protect the software DNS service malicious (malware) that exploits the DNS	
126	Protection against malware must accept reputational domain information malicious	
127	Automatic update of malicious domain reputation lists supported by the manufacturer	
128	The control must validate: the domain, the IP address of the domain, the FQDN and IP address of the authoritative name server of the domain to analyze	

DNS Analytics		
129	Ability to allow the solution to block malicious queries made by persistent advanced threats and malware to sites Command Control (C&C) and botnets	
130	If at any time it is required, the solution must have the capacity to can be added by licensing to the protection solution of DNS analytics behavior proposed for DNS Caching computers you must add the associated destinations to the ex data filtering for the communications to list an RPZ and block communication with those domains. The DNS analytics behavior protection solution proposed for DNS Caching teams must provide commitment indicators (attempts to exfiltrate data) and have the ability to develop through APIs, configure or through a license to issue an action at endpoint solutions to accelerate and automate security responses	
Thread Intelligent Feeds / malware		
131	The solution must allow multiple security feeds, including coexistence of proprietary and 3rd party feeds.	
132	Security feeds must be provided feed with lowest false positive	
133	Security feeds must be provided by centralize service with capacity to add additional feeds selected by the ISP	
134	The vendor must have his own Threat Intelligence unit.	
135	The solution must support event logging in Common Event Format (CEF) format for integrating with SIEM solutions	
136	It must be possible to integrate the DNS solution into the overall security ecosystem using webservices	
137	The solution must be able to support value added services for subscribers (e.g. parental control, security).	
138	The solution has to synchronize and update from Internet, with centralize node.	
139	The solution has to provided a centralize distribution of Security feeds and threat intelligence to all nodes.	
140	The solutions must be able to deliver contextual awareness service and analysis to block threats from a dynamic set of high-risk IP addresses, to Detect malicious activities and sites and IP addresses	
DHCP service features:		
141	Support for high availability of DHCP service	
142	Historical reports of DHCP assignments	
143	Advanced editing of DHCP options	
144	Expansion and division of DHCP networks without loss of configuration information	
145	You must identify the operating system of DHCP clients, without requiring	
146	infrastructure, processes or additional network activity	
147	RFCs for DHCP: 1531, 1534, 1542, 2131, 2132, 3046, 3315, 3925, 4388, 4075,	
148	3898, 3736, 3646, 3633, 3319.	
149	DHCP Fingerprint that allows to recognize the type of device (Windows,	

	MAC OS,	
150	iPad, Android) that connects to the internal network	
151	DHCP Failover support for high service availability	
152	History of DHCP leases.	
Features of the IP Address Management (IPAM)		
153	Integrated IP address management console that can run the DHCP and DNS services if necessary	
154	Track the history of delivered IP addresses	
155	Ability to automatically identify the next available IP address in a network	
156	Network discovery, to find active IP addresses	
157	A team dedicated to the administration of Ips is required, from which they can centralize the administration of the other components of the DNS solution and DHCP proposal	
158	Expansion and division of networks without loss of configuration information	
159	Union and division of networks	
160	Network discovery	
161	Extensible Attributes	
162	Global searches	
163	Recycle bin	
Architecture		
164	The solution must be based on latest purpose-built technology and specific for DNS and related network services	
165	The solution does not have to allow for root access as it has to be based on a fully hardened solution and completely manageable through dedicated and controlled interfaces (GUI, CLI or API).	
166	The appliances must include an embedded and zero-administration distributed database. No need for specific database skills to administer the solution, skills to purge or re-index the database is required. All administrative function must happen automatically inside the system.	
167	The solution must offer a dedicated physical management interface for out-of-band management. This will allow data traffic and management traffic to flow through separate paths and be kept separate.	
168	The solution must integrate a WEB based management interface that allows for all operations on the cluster’s nodes, such as configuration, backup, restore, upgrades, troubleshooting, etc.	
169	Any change applied through the management interface, including the configuration changes to the services (DNS, etc) and the management changes to the operational status of the nodes (IP Address, management passwords, etc) must be propagated to all nodes in real time for immediate availability.	
Resiliency		
170	The solution must guarantee the service continuity through configurations allowing for high availability structures and configurations like IP Anycast.	

171	The solution must allow full Disaster Recovery configurations where in case of disaster the Master function can be easily recovered (single command) guaranteeing all data (configuration and operational) to be maintained and made available from another management node (previously defined).	
172	Within a cluster it must be possible to define an indefinite number of master backup units, each having the complete dataset (configurations and operational statuses) available any time. Each of these Master backup units must be capable of providing DNS services at the same time as running as the (or one of the) Master backup(s).	
173	The solution must allow each node of the solution to be easily configured as high availability pair, implying the use of VRRP to form a unique logical unit from the operational standpoint; all services and functions a single unit offers will have to made available in the same way when configured in HA.	
174	The solution must offer other means to secure service offering, including highly resilient structures (in the cluster or outside), protocol redundancy and protection for a fault against the management unit.	
175	The solution shall offer also protocol failover mechanisms such DNS Primary/Secondary configurations and offer a fully redundant structure through combining all the above mechanisms, all controlled through the unique management interface (GUI).	
176	The solution must provide a mechanism for backing up all data and configurations (possibly in one unique file). The backup must be allowed to run manually but also to be scheduled and sent to external storage systems through standard protocols such as FTP, TFTP, SCP.	
177	The restore mechanism must be made available from the central GUI. Once restoring a configuration that has to be including all data for each remote member. If the member must not be available at restore time it will be retained in the central management unit till the node comes alive.	
178	The cluster must provide log information thorough syslog and audit log outputs to allow administrators to control the operational status and identify operational issues of administrator configurations/operations. Auditlog must describe each and every change an administrator has been making on any of the cluster nodes.	
	General Administration	
179	The central management node (Grid Master, not necessarily a dedicated unit for the function) must maintain a continuous connectivity to all the managed nodes to retrieve also their operational status and keep synchronized all possibly relevant data in a real time fashion.	
180	Each administrative change applied from the cluster management interface (GUI) must be possible to be scheduled for later activation and control.	
181	Software updates and patches must be applicable from the central management interface to all nodes of the cluster. Applying any update/patch must be possible without need to log into any of the cluster's nodes and without need for root access anywhere. In no cases root access have to be allowed.	

182	An upgrade or patch must be possible without loss of configuration data during the process as standard procedure.	
183	The solution must allow to revert back from an upgrade and return to the previous operational configuration status (including old dataset) that was running prior to the upgrade, through a single command issued from the management interface (GUI).	
184	The graphical management interface (GUI) must include an automatic error prevention engine that controls all data being inserted via any of the interfaces available (GUI, CLI, API, etc) to prevent errors from being inserted in the configuration.	
185	The management interface must provide an administrator delegation function to control and limit access (Read-Only or Read-Write) only to the defined subsets of the whole dataset each administrator needs to operate on. All operations must be logged as for any administrator's activity.	
186	The access to the GUI on the Grid Master must be ruled by authentication mechanisms; user access rights can be governed through a local user database or authentication can be provided through external systems such as MS Active Directory, Smart Card, Radius and Tacacs+.	
187	The solution must allow to easily import configuration data via integrated mechanisms in the GUI or via available importing tools.	
188	The solution must offer standard mechanisms to integrate with third party monitoring systems and alerting systems.	
189	The product must be Common Criteria 2 certified EAL2.	
190	To maximize security and audit, the solution does not have to allow root access to the underlying operating system or configuration layer for any reason.	
191	All management changes and controls must be possible from the centralized management interface (GUI) and from that all operational statuses of each node of the cluster must be visible and manageable.	
192	All communications between the Grid Master and the other Members of the cluster must be encrypted; all data transferred from the Master to the nodes has to be verified for correctness prior to being applied in the distributed database. This to guarantee data integrity against each configuration change.	
193	The GUI on the client must communicate with the management node only through secure communication channels (encrypted communication).	
194	Each administrator accessing the GUI must be authenticated and profiled prior accessing the dataset. Smart cards must be supported. Authentication shall be possible via authentication on a local user database or on MS Active Directory, RADIUS and TACACS+.	
Reporting		
195	Reporting must be delivered from a dedicated appliance so that resources to generate reports do not affect protocol delivery of DNS and other functions.	

196	All data needed to generate report must stay within the network. No data has to be exported to third parties in order to produce reports.	
197	The solution must come with rich reporting facilities	
198	Reporting must be preconfigured with a rich set of reports	
199	It must be possible to schedule automatic report generation and distribution by email or ftp	
200	Reporting must have minimal impact on the DNS protocol delivery	
201	Any change applied through the management interface, including the configuration changes to the services (DNS, etc) and the management changes to the operational status of the nodes (IP Address, management passwords, etc) must be propagated to all nodes in real time for immediate availability.	
202	Vendor to provide Solid References within Service Providers customers across the region	

(7) Technical Bid for Firewall Rule Analyzer with NSPM: (either dedicated or in-built)

S No.	Item Description	Compliance (Yes / No)
1	The solution takes accessibility limitations in consideration. The solution is fully usable for color blind person.	
2	The solution supports GrapghQL as API language.	
3	The solution must be able to maintain and visualize a compliance policy matrix with the different security requirements, indicating in the matrix what type of flows are valid between different network zones, to prevent changes from being made that are not in accordance with the company compliance policy. It must be possible to define allowed services and applications (based on App-ID)	
4	If a violation against the compliance policy matrix is detected the solution will be able to send alerts via email and syslog out of the box. Without custom scripting.	
5	The solution must be able to detect changes on the equipment being monitored in near real time. The change detection is done on an event basis and not only periodically.	
6	The solution must be able to keep track of changes of the DFW for NSX-V and NSX-T, and maintain multiple revisions, allowing each change to be easily identified with information.	
7	The solution must present the NSX-T components in a graphical network topology map. This includes the Ditribution FW and Edge services	
8	The solution must be able to track the changes occur to Panorama DAGs which defined by Tags	
9	The solution must be able to support multi-tenancy mode/MSSP including overlapping IPs on one installation. (one central server)	
10	The solution must be able to build L3 topology map automatically, based on the Cisco ACI configuration, including the support of service graph. the topology map must be updated automatically based on service graph configuration.	
11	The solution must be able to analyze and provide the results of a query of traffic flow between 2 Cisco ACI end points including all network and security components, such as VRFs, contracts, external EPGs, E/W traffic and N/S traffic.	

12	The solution must be able to provide generic tools to expand the network topology map. This includes generic route, interface, device, VPN, and L2 transparent FW modeling. The control should be through a GUI.	
13	Ability to view a permissiveness score on firewall rules	
14	Ability to create a hierarchical relationship of zones	
15	Ability to define a network segmentation policy that allows only host-to-host, host-to-subnet, subnet-to-host, or subnet-to-subnet FW rules for zone to zone interaction.	
16	It must be possible to establish a flow of approvals so that each change can be discarded, notified and approved. The system must be able to define several task to approve only the flows the approver is applicable. For example depending on the firewall in question, the criticality of the change or its urgency. The configuration must be done via UI.	
17	The solution must be able to define company processes in a new workflow to request flows. The configuration of advanced workflows must be doable via UI. The solution must be able to have multiple workflows for different process e.g. for different departments. Out of the box support is required, and the ability to add/remove steps via UI.	
18	The solution must be able to support change-window automation for implementing changes in non-working hours for management systems.	
19	The solution must provide a customizable workflow to decommission server. If a server is no longer used the workflow will take the IP addresses as input and will remove the reference in any firewall rule or firewall group.	
20	The solution must provide a customizable workflow to clone the policy of an existing server. If a new server is installed and has the same role as an existing server, the workflow will create a new entry in any firewall rule or firewall group where the refrenced server is used.	
21	The solution must be able to support a fully-automated workflow (Zero touch automation) with an option to change the automation level per step via the UI out of the box.	
22	The solution must be able to close tickets automatically if the requested change has already been implemented, to reduce the workload of users. This feature must be built in. The solution will also automatically document the new ticket information in the existing rule.	
23	Implement changes to Palo Alto and Check Point Firewalls with LDAP groups (browse LDAP directory as part of the Access Request ticket) and provision the changes.	

24	The solution must be able to save or commit changes and the ability to change provisioning behavior (save/commit changes) per ticket	
25	The solution must be able to provision NGFW functions to Panorama through a ticket lifecycle. It is mandatory to support UserID, AppID, ContentID, Tags and FQDN objects	
26	The solution must be able to simulate traffic analysis query, and troubleshoot network connectivity issues with LDAP integration (User-ID). to assess users access and connectivity.	
27	The solution provides capabilities to automatically push change request to the industry leading firewall vendor systems.	
28	The solution must provide end-to-end support for Firewall Manager, including visibility, change tracking and automation.	
29	The solution must be able to automate changes including Security profile groups selection.	
30	The solution must be able to automate IPv6 changes	
31	The solution provides an application driven change process. The application owner can maintain the lifecycle of an application in the solution and create the necessary change request out of this application connectivity documentation.	
32	It is mandatory to validate each application change with a security policy matrix with a zone to zone interaction.	
33	The solution must be able to support application migration and application cloning.	
34	The solution must be able to monitor the application status based on the security policy and network connectivity	
35	The solution must provide a native integration with vulnerability management solutions and correlate network access to network host vulnerabilities to identify exploitable and accessible assets	
36	The solution must be able to modify network access to mitigate contextually exposed vulnerabilities through integrated workflows without requiring customization	
37	The solution must provide reporting capabilities to summarize the vulnerabilities exposed in the network to direct remediation prioritization	
38	The solution must provide a native integration with vulnerability management solutions to retrieve vulnerability scan results, or initiate new scans, and automate risk decisions for access requests based on the results to maintain a state of known risk	
39	The solution must have a native integration with IPAM/ DDI solutions to map stored subnets to network segments to generate accurate network access violations through a network segment to network segment connectivity matrix	

	NSPM – Network Security Policy Management specifications for multivendor Firewalls including L3 Switches, Application Visibility and Network Mapping	
40	The NSPM solution (OEM) should have a local registered presence in India with direct availability of 24x7 support, PS and Development center in India for the min last 1 year. Certificate of InCompany in India is must to be submitted as a documentary proof.	
41	The proposed OEM solution should have a local experience working with at least 5 public sector organizations in India. OEM to furnish end user details on their letterhead.	
42	To streamline Firewall management, the proposed NSPM solution should support an integration with multi-vendor Firewall technologies including Checkpoint, Cisco, Fortinet, Palo-Alto & Juniper and SDN platforms such Cisco ACI & VMWare NSX-T to assess the inline configuration for Risk, Changes, Optimization & Regulatory Compliance (such as ISO 27001, PCI & NIST).	
43	The proposed NSPM solution should have an inbuilt Workflow based ticketing system to automate Firewall changes, all the new Traffic Change Request should be proactively assessed against the risk matrix available out of the box before implementation to avoid Risky & non-compliant Access controls on the Firewalls.	
44	To ensure continuous compliance, the proposed NSPM solution should perform Risk Analysis for integrated Firewalls and should also proactively perform impact analysis before provisioning the rules on the multi-vendor Firewalls.	
45	To Simplify Firewall Rules Clean process & to avoid an outage the proposed NSPM solution should provide detailed report on Rules Usage, Unused Rules, Covered Rules, Time-inactive Rules, Logs without Logging, Disabled Rules, Redundant Rules and Rules without Remarks. For Rules Usage/Unused Rules the proposed solution should allow generating reports based on defined time (last 90 days logs (should be a customizable parameter))	
46	To ensure Risk free network, the proposed NSPM solution should assess Firewalls & Routers/Switches configuration and build an automatic network map and topology for day-to-day connectivity troubleshooting.	
47	To simplify Firewalls access controls management the proposed NSPM solution should automatically name the new Access Controls based on the configured nomenclature.	

48	To ensure strict Firewall Changes documentation the proposed NSPM solution should automatically discover all the Changes which has been implemented “Widely”, “Partially” or “without Change Request” (emergency Changes).	
49	To ensure clean Firewall ACL’s migration from existing Firewall brand to new Firewall brand (as mentioned above) the proposed NSPM solution should have a dedicated change workflow which not only allows automating the Firewall ACL’s migration but should also document each n every step of the migration process from a Compliance & Auditing perspective.	
50	To streamline critical business applications and operations, the proposed NSPM solution should support discovering & mapping of Business Applications and their connectivity flows within the inline Firewall Access Controls based on NetFlow or based on the telemetry’s provided by 3rd party discovery solutions such as Cisco Tetration, Guardicore or Illumio. Min 5 Apps to be supported from day 1 of Implementation.	
51	To provide holistic view of vulnerabilities criticality & to endorse their patching the proposed NSPM solution should integrate with third party VA Scanners like Qualys, Nessus and Rapid7 to map server related vulnerabilities with the discovered/inline business applications.	
52	The NSPM solution should be capable of supporting hybrid cloud environments including on premise, SDN and Public Clouds. The solution should scale to provide security visibility and automated change provisioning capability for cloud native security policy including Azure and AWS.	

(8) Technical Bid for Server Security:

S No.	Item Description	Compliance (Yes / No)
1	Eliminates the cost of deploying multiple software clients with a centrally managed, multi-purpose software agent or virtual appliance	
2	Reduces complexity with tight integrations with management consoles from Trend Micro, VMware, and enterprise directories such as VMware vRealize Operations, Splunk, HP ArcSight, and IBM QRadar	
3	Protects Docker host and containers with Anti-Malware scans and Intrusion Protection	
4	Reduces management costs by automating repetitive and resource-intensive security tasks, reducing false-positive security alerts, and enabling workflow of security incident response	
5	Significantly reduces the complexity of managing file-integrity monitoring with cloud-based event whitelisting and trusted events	
6	Detects vulnerabilities and software via Recommendation Scanning to detect changes and provide protection from vulnerabilities	
7	Provides auto-scaling, utility computing, and self-service to support agile organizations running a software-defined data center	
8	Leverages Deep Security's tight integration with VMware to automatically detect new VMs and apply context-based policies for consistent security across the data center and cloud	
9	Integrates with the latest VMware vSphere and NSX™ versions. Deep Security extends the benefits of micro-segmentation in the software-defined data center with security policies and capabilities that automatically follow VMs no matter where they go	
10	Sends alerts and triggers proactive prevention upon detection of suspicious or malicious activity	
11	Tracks website credibility and protects users from infected sites with web reputation threat intelligence from Trend Micro's global domain reputation database	
12	Identifies and blocks botnet and targeted attack command and control (C&C) communications using unified threat intelligence from Trend Micro's global domain-reputation database	

(9) Technical Specification for DAM:

Sr. No	Specifications	Compliance (Yes/No)
	Architecture	
1	Solution should be appliance based or virtual appliance based.	
2	Does the solution require deployment of agents on the database servers?	
3	If So, There should be only one agent to monitor all DB activities including local DB traffic and network DB traffic	
4	All agents regardless of deployment mode should be managed from the centralized management console	
5	Agents should have only minimal overhead for the production DB servers	
6	Agent should support AIX,HPUX, LINUX, Solaris and Windows platforms	
7	there should not be additional agents required to be installed to monitor and block DB traffic/attacks traffic if required	
8	Solution should not have any 3rd party Software to be installed for agents	
9	Audit trail should be stored within the solution and it should not be stored in any database	
10	Audit trail should be tamperproof and should be stored in encrypted flat files.	
11	Solution component should be managed centrally.	
12	Solution Should support below DB platforms PostgreSQL (open source) Mongo DB (open source) PostgreSQL (enterprise DB) Mongo DB (commercial) Oracle MS-SQL (Microsoft SQL Server) MySQL Teradata Netezza	
	Database Discovery	
1	Solution should discover both new and existing database systems and should map all on the network.	
2	product should provide automated discovery of both new and existing Database tables	
3	Product should keep the historical information about the systems and their configuration.	
4	Product should show changes since the last scan for DB Discovery and configuration	

5	Solution support identification of rogue or test databases	
6	Solution should discover asset management and change management processes	
	Data Classification	
1	The product should perform data discovery and classification	
2	Solution should detect sensitive data types, such as credit card numbers, social security numbers, etc., in database objects	
3	The solution should locate CUSTOM data types in database objects	
	Vulnerability Assessments	
1	Solution should have DataBase vulnerability assessment tests for assessing the vulnerabilities and mis-configurations of database servers, and their OS platforms. OSs and RDBMSs are tested for known exploits and mis-configurations.	
2	Solution should have a comprehensive list of pre-defined assessment policies and tests to address PCI-DSS, SOX, and HIPAA requirements. Vulnerabilities specific for SAP, Oracle EBS, and PeopleSoft databases can also be detected. In addition, the following tests should be included: - Latest patches and releases installed - Changes to database files - Default accounts and passwords - Newly created/updated logins - Remote OS authentication enabled - Escalated user privileges granted	
3	Should be able to add custom assessments to the solution?	
4	Solution should support user created scripts for assessment tests.	
5	The product should identify missing patches	
6	The solution verify that default database accounts do not have a “default” password	
7	The product should be used to measure compliance with industry standards and regulations	
	Vulnerability Assessment Result Analysis and Reporting	
1	The product should present a view of risk to data – by vulnerability and the sensitivity of the data	
2	Solution should have DataBase vulnerability assessment tests for assessing the vulnerabilities and mis-configurations of database servers, and their OS platforms. OSs and RDBMSs are tested for known exploits and mis-configurations.	

3	Solution should have a comprehensive list of pre-defined assessment policies and tests to address PCI-DSS, SOX, and HIPAA requirements. Vulnerabilities specific for SAP, Oracle EBS, and PeopleSoft databases can also be detected. In addition, the following tests should be included: - Latest patches and releases installed - Changes to database files - Default accounts and passwords - Newly created/updated logins - Remote OS authentication enabled - Escalated user privileges granted	
4	The Solution should have pre-defined reports.	
5	the product should support custom report generation.	
6	The product should compare the results of a discovery, classification or assessment job with a previous run	
7	Should have an option to distribute reports on demand and automatically (on schedule)	
	Remediation (optional : for future requirement)	
1	The product can be upgraded to for mitigating risk to sensitive data stored in databases?	
2	Should have an option to upgrade the product to actively prevent attempts to exploit known vulnerabilities	
3	The solution can be upgraded to offer virtual patching capabilities (protecting the database from known vulnerabilities without deploying a patch or script on the system)	
	Database Activity Monitoring	
1	Solution Should have Appliance/virtual appliance solution to monitor network based DataBase activity and should have agents to monitor Local DB activity	
2	Should product employ a centralized appliance	
3	Solution should provide for centralized control of collected information	
4	Should have DBMS product to be used as part of the appliance package to store configuration and alert logs, not for storing Audit data	
5	The solution should support high-availability	
6	Product should be able to installed in Sniffing mode or Inline mode.	
7	Solution should have built in bypass(fail open) for inline mode	
7	Solution should support below DataBases Oracle, MS SQL, DB2, Informix, Sybase,MySQL, Teradata,Netezza	
8	The solution should not use the native database audit functionality.	
9	the Solution should not employ transaction log auditing?	
10	Should be able to integerate with leading SIEM tools	
11	The product should have means to archive and restore data	
12	The agent should not require a reboot after installation/configuration	

13	The solution should not require any changes to monitored database and/or application	
14	The Solution should not require a database restart after installation/configuration?	
15	The audited data transferred between the agent and the appliance should be through an Encrypted channel	
16	The solution should capture before and after image of data that is being manipulated	
17	Product should identify differences in baseline user activity.	
18	The solution should capture Select activity by user/role	
19	The solution should capture update, insert, delete (DML) activity by user/role	
20	The solution should capture schema/object changes (DDL) activity by user/role	
21	The solution should capture manipulation of accounts, roles and privileges (DCL) by user/role	
22	DAM Should monitor privileged operations including both SQL and Protocol level operations be monitored.	
23	DAM Should monitor MS SQL statements where caching is used	
24	DAM solution be able to monitor activities at new DB interface/ connector created by any user/ system without any manual intervention	
25	Solution should Identify abnormal Data Based access based on profiling.	
26	Solution should be able to Identify the real end-user for enterprise application activity.	
27	Solution should not be based on timed sampling of the database shared memory. This results in lost traffic when the load is high.	
28	Solution should use agents only for monitoring the data base traffic. Traffic analysis and policy engines should not run on agents, if so this will introduce overhead to the database server.	
29	Solution should have Data Base profiling feature to identify abnormal DB activities.	
30	Solution should integrate with Web Application firewall to track application end users.	
31	Solution should should have same console to manage(create policies, DAM audit reports, WAF reports, alerts etc) both DAM & WAF solutions. This will help to have single administrator to manage both solutions.	
	Alerting and Blocking Capabilities	
1	The solution should provide automated, real-time event alert mechanism	
2	The solution should have an option to upgrade to database attack in real-time	
3	The solution should monitor privileged users	

4	The solution should have an option to upgrade to block privileged users activity if required	
5	The Solution should monitor for all DB attacks like SQL injection and alert despite the traffic is not audited.	
6	The Solution should have an option to upgrade to block DB attacks like SQL injections in real time.	
7	Solution should not use Data Base triggers to block the traffic.	
8	Solution should Identify and block non-SQL access such as export table direct.	
9	Solution should have an option to integerate with anti-malware solution to block infected sysems accessing Data Base Servers.	
10	The solution should 100% monitor the DB traffic for all DB violation and attacks despite the traffic is not being audited	
	Reporting	
1	Solution should have packaged reporting capabilities	
2	product should support use of pre-configured policies/reports (PCI, SOX, HIPAA) for ensuring regulatory compliance	
3	Product should have a functionality to assist with security event forensics	

(10) Technical Specification for Network Inspector

Sr No	General Specifications	Compliance (Yes / No)
1	The Network Inspector should be a physical network appliance that should monitor 360 degrees of the network to create complete visibility into all aspects of targeted attacks, advanced threats, and ransomware.	
2	The Network Inspector should Inspect all network content and monitor all traffic across physical and virtual network segments, all network ports, and over 100 network protocols to identify targeted attacks, advanced threats, and ransomware. It should have agnostic approach to network traffic and detect targeted attacks, advanced threats, and ransomware from inbound and outbound network traffic, as well as lateral movement, C&C, and other attacker behavior across all phases of the attack kill chain.	
3	The Network Inspector should utilize extensive detection techniques such as utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior	
	Platform	
4	Hardware Appliance must be able to handle minimum of 1 Gbps of traffic capacity for inspection	
5	Hardware must have minimum 4 x 1G Ethernet ports	
6	Hardware Appliance should have out of band management port	
7	Hardware should have minimum capacity of 1 TB	
8	Hardware Appliance should be supplied with redundant Power Supply.	
9	The proposed Hardware should be rack mountable appliance	
10	The proposed solution must be available as on premise physical appliances with sandboxing capability	
	Advanced Threat Detection	
11	Proposed ATP solution should perform advanced network detection and analysis of the enterprise's internal/External network data.	
12	The proposed solution should have the ability to support out-of-band detection	
13	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance	
14	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, IPS etc	

15	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	
16	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	
17	The Proposed solution should be able to detect communications to known command and control centres.	
18	The proposed solution should be able to detect reputation of URL being accessed	
19	The proposed solution should support at least 100+ protocols for inspection	
20	Proposed Solution should be validated by 3rd Party like NSS as a Breach Detection System (BDS) with minimum detection rate 96% or above.	
21	The Proposed solution should support Microsoft O/S environments etc, for Sandboxing	
22	Sandbox must have the ability to simulate the entire threat behavior.	
23	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	
24	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files	
25	The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing	
26	The proposed solution should support Multiple protocols for inspection. Example:- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	
27	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	
28	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	
29	The Proposed solution should be able to monitor more than 100 Protocols & all (65535) ports.	
	Management and Reporting	
30	The proposed solution shall support CLI, GUI/Web based administration Console.	
31	The proposed solution shall support Remote administration using SSH/HTTPS	
32	The proposed solution should provide an intuitive Dashboard that offers real time threat visibility and attack characteristics.	
33	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	

34	The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats	
35	Should support receiving suspicious files from the server security for generating real time Threat intelligence for server protection and to achieve Advanced Threat defense i.e IOCs must be shared between the Network Inspector and the server security for achieving advanced Threat Defense.	

Annexure – 4D: Technical Solution Requirements for Email & Archival Solution:

S. NO	Item Description	Compliance (Yes / No)
1	The Bidder shall be responsible for the implementation of the Centralized Mail Messaging Solution in Single Domain architecture with High Availability.	
2	The Bidder shall be responsible for Supply, Installation, Upgradation, Integration, Rollout, Operationalization, failover testing, and Maintenance of total solution for the implementation of MS Exchange 2016/2019 based Mail Messaging Solution comprising Hardware, Software, Operating System and Data Base at the proposed Data Centre.	
3	Complete end-to-end implementation of the system including hardware, software etc.	
4	Bidder shall be responsible for setting up infrastructure for publishing ECGC email services to the Internet and securing the same w.r.t messaging services.	
5	The Mail & Messaging Infrastructure would be based on Microsoft Windows Server 2016 or 2019 (Standard or Datacenter Editions) operating systems with Exchange 2016 or 2019 Server (Enterprise Edition recommended) with membership in an Active Directory Domain.	
6	Bidder will configure the mailing solution with the existing TrendMicro IMSS server (Gateway Server).	
7	The Bidder shall be responsible for the migration of all existing Zimbra database and mail exchange records to the proposed MMS system. During migration of database and other records, the bidder shall ensure to minimize the end-user impact as much as possible. If there is any issue involved in migration bidder shall discuss the same with ECGC and will plan accordingly. There should not be any data loss during migration. Further Bidder shall be responsible for deploying the Exchange Edge server in the existing box.	
8	The Bidder will be responsible for the management of the complete Mail Messaging Infrastructure solution for the next 5 years.	

9	The bidder shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams and other reports etc. All such documents shall commence only after the same is approved by ECGC.	
10	The bidder shall review the current mail messaging policy of the Bank and should recommend the best practices to implement and rollout the same within the ECGC.	
11	The bidder shall provide detailed drawing of the installed setup after completion of the project. This will also include the printout of important configuration settings of the servers.	
12	The bidder should provide a detailed plan on the support for the Mail Messaging Solution to maintain the uptime of 99.5% to be calculated on monthly basis.	
13	The Bidder shall be responsible for all patches/updates required in the offered solution for smooth installation of Exchange 2016/2019 without any extra cost to the Bank.	
14	The ECGC has present requirement of 800 mailboxes approx., which may increase in future.	
15	Active Directory Services:	
	Configuring & deploying a proper domain architecture as per design	
	Defining policies for administration, security etc.	
16	The average size of a mailbox should be 20 GB.	
17	The proposed messaging solution should provide archiving and journaling capabilities for all mail boxes on the server side to be used by Compliance officer, Auditors and Administrator for Audit and Backup/restore purpose.	
Email Archival Solution		
18	Support end-user archiving for Microsoft Exchange 2016/2019 platform and other email platforms	
19	Support Global deduplication of Archived Content (i.e. email, files, sharepoint, IM, databases.)	
20	Support Policy-based management and workflow to automate archiving processes and take	
21	control of data sprawl	
22	Supports virtualization infrastructure for flexible deployment without additional hardware	

23	Enable roles-based search and access for self-service users to search, preserve, review and export	
24	electronically-stored information and messages	
25	Have in-build data classification	
26	The solution should support access to Archive mailbox both from email client and Web Based email access.	
27	Integrated content archiving for Email systems and PST files, File servers, Microsoft SharePoint, Enterprise content management systems, Databases and ERP systems	

Annexure – 4E: Technical Solution Requirements for MSP Services

(i) Technical Requirement for MSP Services:

Sr. No.	ONSITE Support Services Requirement	No of Resources proposed	Role/ Designation	(mention dedicated/ shared)	Remarks (attach solution
1	Central Helpdesk at Mumbai including management of user issues (onsite and remote) like PC & printer configuration, mail client configuration, antivirus installation and update, proxy settings, AD issues, password issues etc.				
2	Remote Helpdesk (Hyderabad, Ahmedabad, Kolkata, Delhi, Bangalore, Chennai, Tirupur)				
3	Mail Management				
4	Security Monitoring and Management (SOC)				
5	Antivirus Management				
6	Firewall Management				
7	Server, OS, and System Management				
8	IT Assets Management, configuration Management, Asset Call logging, monitoring, movement tracking, closure				
9	Vendor Management				
10	Project Management & SLA Management				
11	User / Employee Support				
12	Backup / Archival/ Replication management				
13	Support /Maintenance of any other product/ services under SI's scope of this tender (add as line item)				

(ii) Technical Requirement for SI for MSP Services:

Sr No	Description	Details
1	Bidder should have experience in BFSI and Insurance sector for infra and Application support	<Please attach evidences>
2	Bidder should provide customer references for Managed Services for Infra and Application support having order value more than 20 lakhs in (Private/PSU/Central work Govt/State Govt. or any other Organisation or agencies) in India (Attach as many references)	<Please attach evidences, order value, copies>
3	Bidder should have Expertise in Database support (3 customer references required) and have executed at least one order of 70 Lakhs Plus in the last 3 years.	<Please attach evidences, order value, copies>
4	Project / SLA Management, Monitoring / Governance Framework proposed	<Please attach >
5	Bidder Should have experience of providing Support in 3rd Party data center	<Provide Customer reference>
6	SI shall submit detailed Support strategy for MSP services	<Provide detailed strategy>

…….

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 5A : Price / Commercial Bid Format for UAT SETUP

SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF HARDWARE FOR ECGC SMILE PROJECT

(Must be submitted in the 3rd **sealed envelope**)

COMPANY NAME: _____

ADDRESS:

_____

CONTACT PERSON: _____ PHONE NUMBER: _____

EMAIL: _____ WEB SITE:

_____

We submit our Price/commercial bid (fees) for the proposed assignment as under for <u>UAT Environment</u>

Components	**Descriptions**	**Quantity**	**Unit Price**	**Total**
HCI with Virtualisation layer		14		
UTM/ IPS/IDS		1		
WAF + GSLB + SLB		1		
Internal Firewall		1		
Layer 3 Switch		2		
Distribution Switch (TOR) compatible with HCI		2		
DDI		1		
Firewall Rule Analyzer		1		
Server Security	(Quantity as per solution requirement)			

DAM	(Quantity as per solution requirement)	1		
Network Inspector		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.**

……

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 5B : Price / Commercial Bid Format for DC SETUP

SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF HARDWARE FOR ECGC SMILE PROJECT

(Must be submitted in the 3rd **sealed envelope**)

COMPANY NAME: _____

ADDRESS:

_____

CONTACT PERSON: _____ PHONE NUMBER: _____

EMAIL: _____ WEB SITE:

_____

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

(I). DC Environment

Components	**Descriptions**	**Quantity**	**Unit Price**	**Total**
HCI with Virtualisation layer		25		
UTM/ IPS/IDS		1		
WAF + GSLB + SLB		1		
Internal Firewall		1		
Layer 3 Switch		2		
Distribution Switch (TOR) compatible with HCI		2		
DDI		1		
Firewall Rule Analyzer		1		

Server Security		1		
DAM		1		
Network Inspector		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). Datacenter 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				
			Grand Total	

(III). Mail, AD and Archival Solution:

S.No	Descriptions	No of Mailbox	cost	Total
1	Mailing solution for 800 mail boxes	800		
2	Archival solution			
3	Hardware and software Required for			

	AD implementation (attach BOM as Annexure with solution details)			
4	Hardware and software Required for mailing (attach BOM as Annexure with solution details)			
5	Hardware and software Required for Archival solution (attach BOM as Annexure with solution details)			
4	Implementation and Commissioning charges			
5	Conversion and migration of email backups to archival solution			
			Grand Total	

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

……

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id

Annexure – 5C : Price / Commercial Bid Format for MSP

SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF HARDWARE FOR ECGC SMILE PROJECT

(Must be submitted in the 3rd **sealed envelope**)

COMPANY NAME: _____

ADDRESS:

_____

CONTACT PERSON: _____ PHONE NUMBER: _____

EMAIL: _____ WEB SITE:

_____

We submit our Price/commercial bid (fees) for the proposed assignment as under for <u>Managed Services</u> as Managed Services Provider

(I). Service wise Cost

Sr. No.	ONSITE Support Services	Yearly Cost (INR)	Total Cost (5 Years) (INR)	Remarks
1	Central Helpdesk at Mumbai including management of user issues (onsite and remote) like PC & printer configuration, mail client configuration, antivirus installation and update, proxy settings, AD issues, password issues etc.			
2	Remote Helpdesk (Hyderabad, Ahmedabad, Kolkata, Delhi, Bangalore, Chennai, Tirupur)			
3	Mail Management			
4	Security Monitoring and Management (SOC)			
5	Antivirus Management			
6	Firewall Management			
7	Server, OS, and System Management			
8	IT Assets Management,			

	configuration Management, Asset Call logging, monitoring, movement tracking, closure			
9	Vendor Management			
10	Project Management & SLA Management			
11	User / Employee Support			
12	Backup / Archival/ Replication management			
	Support /Maintenance of any other product/ services under SI's scope of this tender (add as line item)			
	TOTAL			

**** Taxes on Actuals**

(II). MSP Services Breakup: Average resource-wise Cost for managed services

(Please incorporate additional line items/ heading as per your requirement)

Sr. No.	Support Requirement	No of Resources (mention dedicated/ shared)	Role/ Designation	Average Monthly cost per resource	Remarks
1	Central Helpdesk at Mumbai including management of user issues (onsite and remote) like PC & printer configuration, mail client configuration, antivirus installation and update, proxy settings, AD issues, password issues etc.				
2	Remote Helpdesk (Hyderabad, Ahmedabad, Kolkata, Delhi, Bangalore, Chennai, Tirupur)				
3	Mail Management				
4	Security Monitoring and Management (SOC)				
5	Antivirus Management				
6	Firewall Management				
7	Server, OS, and System Management				
8	IT Assets Management, configuration Management,				

	Asset Call logging, monitoring, movement tracking, closure				
9	Vendor Management				
10	Project Management & SLA Management				
11	User / Employee Support				
12	Backup / Archival/ Replication management				
13	Support /Maintenance of any other product/ services under SI's scope of this tender (add as line item)				
	TOTAL				

Terms and Conditions:

1) The above quoted fee is inclusive of all expenses. taxes excluded.

2) We undertake to deliver all the deliverables as envisaged in the proposal / agreement and complete the assignment within the time frame stipulated in the RFP document.

3) ECGC Ltd will deduct tax (TDS) while releasing payment, if applicable as per the provisions of Income Tax Act, and all other applicable taxes, levies, cess etc.

4) ECGC reserves the right to negotiate and change the milestones / payment schedule / percentages with the successful bidder.

5) Provide Cost for each role (Program Manager, Site In-charge, Desktop Engineer, Call Coordinator, System Administrator etc. as required)

6) Indicate support structure for onsite resources dedicated or shared across services

---

Signature of the Authorized Signatory of Company

Name:

Designation:

Contact no. (Mobile):

Email Id:

Company Seal:

Annexure – 6 : Proforma Bank Guarantee For Performance

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

IN CONSIDERATION OF ECGC LIMITED, a company incorporated under the Companies Act 1956 and having its registered office at 10th Floor, Express Towers, Nariman Point, Mumbai 400021 (hereinafter referred to as the "the Purchaser" 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 placed an order on Messers..... a partnership firm / a company registered under the Companies Act, 1956 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 order No..... dated ..... (hereinafter called "the order" which expression shall include any amendments / alterations to "the order" issued by "the Purchaser") for **REQUEST FOR PROPOSAL FOR SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF BACKUP SOLUTION AT ECGC's DC & NDC SITES** as stated in the said 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 order and the Purchaser 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 Purchaser 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 Purchaser 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 Purchaser 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 Purchaser on account thereof and we waive in the favour of the Purchaser 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 Purchaser 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 Purchaser 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 Purchaser that the Purchaser 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 Purchaser 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 Purchaser or any indulgence by the Purchaser 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 Purchaser 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@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-02/IT/05/2019

The following persons are hereby authorized to attend the bid opening on _____(date) in the tender for **"REQUEST FOR PROPOSAL FOR SUPPLY, INSTALLATION, CONFIGURATION & COMMISSIONING OF BACKUP SOLUTION AT ECGC's DC & NDC SITES**" 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_____

(Company 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 is done before the ECGC Auditors following internally laid down audit process and in view of COVID-19 situation, the physical presence of bidders for attending the bids opening may be dispensed with.

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 "-------") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns a company incorporated under the Companies Act, 1956 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 …….(address) 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 means 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.
Provided always that notices to the ECGC shall be served on the Risk Management Division (RMD) in the ECGC's Head Office at Mumbai by Registered post & email.

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 INSURANCE COMPANY

b) SIGNED SEALED & DELIVERED BY THE WITHIN NAMED (BIDDER)

_____

_____

In the presence of

Witness : 1_____

Witness: 2_____

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 commercial bid.

Sr. No.		Weightage	Breakup
A	SI Capabilities (as per Qualification Criteria Scoring)	100	
B	Data Centre Partner Specification	100	
C	SMILE - HCI Solution	200	
D	Data Centre Security & Nw Solution	150	
1	UTM		40
2	Server load balancer, WAF & GSLB		30
3	Internal Firewall		20
4	L3 Switch		20
5	TOR Switch		5
6	DDI		5
7	Firewall Rule Analyzer		5
8	Server Security		10
9	DAM		10
10	Network Inspector		5
E	Mailing Solution	50	
F	MSP Services Scoring	100	
G	Overall Solution	100	
	Total Score	800	

** The marks received out of 800 will be reduced to out of 100 marks.

** Reduce marks to out of 100 = 100/800 * Score obtained

Annexure – 12 : Undertaking to ensure standards of integrity

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 Request for Proposal 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 Request for Proposal."