

Tele: 23385536  
Reply should be addressed to  
Director (IT)

**TATRAKSHAK MUKHYALAYA**  
Coast Guard Headquarters  
National Stadium Complex  
New Delhi – 110001

Quoting: CGHQ/IT/TAPPS/2018-19

16 Jan 19

**INVITATION OF ONLINE BIDS FOR OPENTENDER ENQUIRY**  
**NO.CGHO/IT/TAPPS/2018-19 DESIGN, DEVELOPMENT, IMPLEMENTATION**  
**AND SUPPORT FOR SECURE CHAT WITH SECURE APPLICATION CONTAINER**  
**(PROJECT TAPPS) - INDIAN COAST GUARD**

Dear Sir/Madam

1. **"Online bids" (Under two bid system)** are invited by the **Directorate of IT, Coast Guard Headquarters** for supply of items listed in **Part II** of this RFP. **Manual bids shall not be accepted. Tenders from black listed/ banned firms shall not be accepted. Tender document** can be viewed and downloaded from **Indian Coast Guard web site [www.indiancoastguard.gov.in](http://www.indiancoastguard.gov.in) (for reference only)** and **CPPP site <https://eprocure.gov.in/eprocure/app>** as per the **schedule given in CRITICAL DATE SHEET** mentioned below:-

**CRITICAL DATE SHEET**

<b>SL.</b>	<b>DESCRIPTION</b>	<b>DATE &amp; TIME</b>
(a)	Published Date	16 Jan 2019 (1600 HRS)
(b)	Bid Document Download / Sale Start Date	16Jan 2019 (1600 HRS)
(c)	Clarification Start Date	16 Jan 2019(1600 hrs)
(d)	Clarification end date	22 Jan 2018 (1430 hrs)
(e)	Pre-bid meeting	22 Jan2018 (1430 hrs)
(f)	Bid submission start date	17 Jan 2019(1200 hrs)
(g)	Bid Document Download / Sale End Date	07 Feb 2019 (1000 hrs)
(h)	Bid Submission End Date	07 Feb 2019 (1200 hrs)
(j)	Technical Bid Opening Date	08 Feb 2019 (1430 hrs)
(k)	Opening of Commercial Bids	Will be intimated in due course after technical evaluation by TEC

2. The address and contact numbers seeking clarifications regarding this RFP are given below:-

The Director General  
{for Director (IT)}  
Coast Guard Headquarters  
National Stadium Complex, New Delhi-110001  
Tele: 011-23385536, Fax: 011-23388090

a. Part I- Contains General Information and Instructions for the Bidders about the RFP such as the time, place of submission and opening of tenders, Validity period of tenders, etc.

b. Part II - Contains essential details of the items/services required, such as the Schedule of Requirements (SOR), Technical Specifications, Delivery Period, Mode of Delivery and Consignee details.

c. Part III - Contains Standard Conditions of RFP, which will form part of the Contract with the successful Bidder.

d. Part IV - Contains Special Conditions applicable to this RFP and which will also form part of the contract with the successful Bidder.

e. Part V - Contains Evaluation Criteria and Format for Price Bids.

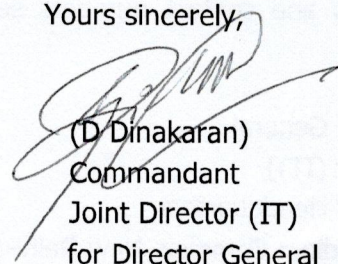
4. This RFP is being issued with no financial commitment and the Buyer reserves the right to change or vary any part thereof at any stage. Buyer also reserves the right to withdraw the RFP, should it become necessary at any stage.

5. You are requested to comply with all the terms and condition mentioned in the RFP and certificate in this regard is to be endorsed on the quote submitted by your firm. Relaxation/deviation of terms/conditions if any, should be clearly brought out for consideration, however acceptance of same will solely be at discretion of Coast Guard. Part I, II, III, IV & V of the RFP are enclosed herewith. Abbreviations & Terminologies to be read as per **Appendix-'L'** and general instructions for online bid-submission as per **Appendix-'K'**.

6. Para marked with "Blank" will not be considered as part of RFP. Bid documents may be scanned with **100 dpi with black and white option, in PDF format** which helps in reducing size of the scanned document. **Bids shall be submitted online only at CPPP website: <https://eprocure.gov.in/eprocure/app>.**

7. Tenderer/Contractor are advised to follow the instructions provided in the 'Instructions to the Contractors/Tenderer for the e-submission of the bids online through the Central Public Procurement Portal for e-Procurement at **<https://eprocure.gov.in/eprocure/app>**'.

Yours sincerely,



(D. Dinakaran)  
Commandant  
Joint Director (IT)  
for Director General

- (a) **Enclosure-I** : Part I - General Information
- (b) **Enclosure-II** : Part II - Essential Details of Items/ Services Required
- (c) **Enclosure-III** : Part-III - Standard Conditions of RFP
- (d) **Enclosure-IV** : Part-IV - Special Conditions of RFP
- (e) **Appendix-'A'** : Functional Requirements
- (f) **Appendix-'B'** : Non-Functional Requirements
- (g) **Annexure-'I' of Appendix-B** : Technical Specifications
- (h) **Appendix-'C'** : Covering Letter to Bid Submission& Bid Check-off List
- (j) **Appendix-'D'** : Covering Letter to Technical Bid
- (k) **Appendix-'E'** : Technical Bid Compliance Sheet
- (l) **Appendix-'F'** : Covering Letter to Commercial Bid
- (m) **Appendix-'G'** : Commercial Bid Format
- (n) **Appendix-'H'** : PQ POC Test
- (q) **Appendix- 'J'** : QCBS for Product and Vendor
- (r) **Annexure-'I' of Appendix-'J'** : POC for Secure Chat Software
- (s) **Annexure-'II' of Appendix-'J'** : POC for Unified Endpoint Management
- (t) **Appendix- 'K'** : Profile of Prime Bidder and Consortium of Vendors
- (u) **Appendix- 'L'** : Instructions for Online Bidders
- (v) **Appendix- 'M'** : Abbreviations & Terminologies

## **PART I – GENERAL INFORMATION**

### **1. Last date and time for depositing the Bids: As per critical date sheet.**

The online Bids (both technical and Commercial, in case two bids are called for) should be uploaded as per this RFP by the due date and time. The responsibility to ensure this lies with the Bidder.

**2. Manner of depositing the Bids:** Online Bids should be scanned and uploaded before due date and time. Late tenders will not be considered. No responsibility will be taken for technical delay or not uploading of bids or Bid documents. Bids sent by FAX or e-mail will not be considered. Samples and EMD to be deposited manually at addressed mentioned in para 2 ibid before opening of Technical bid.

### **3. Time and date for opening of Bids: As per critical date sheet.**

(If due to any exigency, the due date for opening of the Bids is declared a closed holiday, the bids will be opened on the next working day at the same time or on any other day/time, as intimated by the buyer).

### **4. Address for submission of EMD: Directorate of IT, CGHQ**

### **5. Place of opening of the Bids: CGHQ (Directorate of IT).**

### **6. Two-Bid system:**

(a) The case is being processed on two-bid system and, the technical bids shall be opened as per critical date sheet mentioned in this tender document. The evaluation of technical Bid based on requisite documents received online by the tenderers will be carried out by a board of officers. The details of firms found compliant after TEC evaluation will be uploaded on the Central Public Procurement Portal (<https://eprocure.gov.in/eprocure/app>).

(b) The Commercial Bids of only those Bidders whose technical bids meet all the stipulated (Technical) requirements shall be opened. The date of opening will be intimated to the Bidders through Central Public Procurement Portal(<https://eprocure.gov.in/eprocure/app>).

**7. Forwarding of Bids –** Bids should be prepared, signed, scanned and uploaded by the Bidders on their original memo / letter pad. The copies of PAN No, TIN No, CST & VAT, bank details and other enclosures as per part II of RFP and are to be signed/self-attested and scanned with 100 dpi in black and white option in PDF format.

### **8. Details of Pre-bid Meeting: -As per critical date sheet.**

A pre-bid meeting will be held to answer any queries or clarify doubts on RFP and submission of proposals. The authorized representatives are requested to attend. Particulars of personnel (only Indian nationals) attending the pre bid meeting is to be communicated for necessary arrangements at least two days in advance.

**9. Clarification regarding contents of the RFP:** A prospective bidder who requires clarification regarding the contents of the bidding documents shall notify to the Buyer in writing by the clarifications as per critical date sheet at address at mentioned above.

**10. Modification and Withdrawal of Bids:** The Bidder may modify (resubmit) his bid online after submission, as per the provisions available on the portal. No bid shall be modified after the deadline for submission of bids.

(a) If bidder desires to withdraw before bid submission closing date/time, he may do so **online** in the portal. EMD (in case) submitted in physical form shall be returned offline. However, the cost of the tender will not be refunded to the firm.

(b) No bid may be withdrawn in the interval between the deadline for submission of bids and expiry of the period of the specified bid validity.

**11. Clarification regarding contents of the Bids:** During evaluation and comparison of bids, the Buyer may, at its discretion, ask the bidder for clarification of his bid. The request for clarification will be given in writing and no change in prices or substance of the bid will be sought, offered or permitted. No post-bid clarification on the initiative of the bidder will be entertained.

**12. Rejection of Bids:** Canvassing by the Bidder in any form, unsolicited letter and post-tender correction may invoke summary rejection with forfeiture of EMD. Conditional tenders will be rejected.

**13. Unwillingness to quote:** Bidders unwilling to quote should ensure that intimation to this effect reaches by fax/e-mail before the due date and time of opening of the Bid, failing which the defaulting Bidder may be delisted for the given range of items as mentioned in this RFP.

**14. Validity of Bids:** The Bids should remain valid for **90 days** from the date of opening of tenders from the last date of submission of the Bids.

**15. Earnest Money Deposit:** -Bidders are required to submit Earnest Money Deposit (EMD) for amount of **Rs15,00,000.00 (RupeesFifteen lakh only)** in favour of "PCDA(N), Mumbai". The EMD may be submitted "**manually**" on or before opening of technical bid in the form of an Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any of the public sector banks or a private sector bank authorized to conduct government business as per Form DPM-16 (Available in MoD website and can be provided on request). EMD is to remain valid for a period of forty-five days beyond the final bid validity period. EMD of the unsuccessful bidders will be returned to them at the earliest after expiry of the final bid validity and latest on or before the 30<sup>th</sup> day after the award of the contract. The Bid Security of the successful bidder would be returned, without any interest whatsoever, after the receipt of Performance Security from them as called for in the contract. EMD is not required to be submitted by those Bidders who are registered with the Central Purchase Organization

(e.g. DGS&D), National Small Industries Corporation (NSIC) or any Department of MoD or MoD itself. The EMD will be forfeited if the bidder withdraws or amends impairs or derogates from the tender in any respect within the validity period of their tender. Hard Copy of original instruments in respect cost of earnest money be delivered to the Director General, Coast Guard Headquarters, National Stadium, New Delhi- 110 001 on or before bid opening date/time as mentioned in critical date sheet

## **PART II – ESSENTIAL DETAILS OF ITEMS/SERVICES REQUIRED**

### **1. Schedule of Requirements** – List of items / services required is as follows:-

(a) Design, development, implementation and support for **Secure Chat with Secure application container (Project TAPPS)** based on proven software including supply of Secure application container (Unified Endpoint Management-UEM) software licenses (10,000 Devices) and private cloud IT infrastructure with hardware/ software as required. Secure Chat application to be secured with virtual Next Generation Firewall (NGFW) with Web Application Firewall (WAF). Project to **be implemented on turn-key basis** and vendor to include all required hardware/ software as required. Selection of Bidder shall be based on QCBS method as elaborated in **Appendix-'J'**.

(b) Information security audit of complete implementation including Secure Chat software and other IT infrastructure by CERT-IN empaneled vendor

(c) Secure Chat Software Warranty for 01year from final GoLive and 02 year All Inclusive Annual Maintenance Support (AIAMC) including onsite manpower support. Other OEM hardware/ software to be supplied with 03 year warranty with 24x7 support.

(d) **Preliminary Examination of Bids:** - The Buyer will examine the bids to determine whether they are complete, whether the documents have been properly signed, and whether the bids are generally in order. Any bids found to be non-responsive for any reason or not meeting any criteria specified in the tender, will be rejected by the Buyer and shall not be included for further consideration. Initial Bid scrutiny will be held and bids will be treated as non-responsive, if bids are:

- (i) Not submitted in format as specified in the tender document
- (ii) Received without the Letter of Authorization (Power of Attorney)
- (iii) Found with suppression of details
- (iv) With incomplete information, subjective, conditional offers, and partial offers submitted
- (v) Submitted without the documents requested
- (vi) Non-Compliant to any of the clauses mentioned in the tender
- (vii) With lesser validity period
- (viii) Without EMD

### **(e) Prequalification Criteria for Prime Bidder & Consortium Partners:**

(i) Package-A: **Secure Chat software application:** Design, development, implementation and support for Secure Chat application for ICG

(ii) Package-B: **Supply, implementation of Secure Application Container:** Supply of software licenses - 10,000 Nos. and **IT infrastructure to host Secure Chat application at ICG Data Center:** Supply, deployment and support of Enterprise grade Private Cloud IT infrastructure along with necessary support

(iii) Consortium members may provide Package-A or B respectively

Sl.	Prequalification Criteria	Supporting Documents	Doc. Provided (Y/N)
<b>Section-I: Prime Bidder</b>			
(i)	The bidder must be incorporated and registered in India under the Indian Companies Act 1956/ LLP Act 2008 / Partnership Act 1932 and should have been operating for the last five years as on the date of publishing of Tender/ RFP notice (including name change/impact of mergers or acquisitions).	Certificate of Incorporation / Copy of Registration Certificate (s)	
(ii)	The Bidding firm must be a positive net-worth making with annual turn-over of minimum of Rs.05 Crore in the last financial year (2017-18) and overall turn-over of minimum Rs. 04 Crore in the last three financial years: (2017 – 2018, 2016 – 2017 & 2015 – 2016)	Certificate from CA firm / P&L statement and Balance sheet approved by the auditor	
(iii)	Should provide atleast two of three services of (1) Secure Chat application, (2) Secure Application Container and (3) IT infrastructure implementation	(a) Should submit authorised partner certificates from respective OEMs for services (2) & (3)  (b) Should provide deployment details of Secure Chat and reference contact official for (1)	
(iii)	<p>1. During last 05 years ending last day of month previous to the one in which applications are invited:-</p> <p>The Prime Bidder must have successfully completed 02 of following 03 projects in India.</p> <p>(a) IT infrastructure implementation including Server/ storage of minimum 03 projects. Atleast 01 of the should be successful live and currently supported in Central Govt./PSU with Completion certificate within last 05 years. Should have MAF for IT infrastructure for current ICG scope</p> <p>(b) Should have implemented Cloud/ Enterprise grade systems other than hardware of minimum 03 projects. Atleast</p>	<p>Completion certificate (GO-Live / Implementation) with date and</p> <p>1. Work order with order value detailing the scope.</p> <p>(OR)</p> <p>2. Agreement copy defining the scope &amp; value.</p> <p>Also provide client reference detailing Name, Designation, Phone and Email ids.</p>	



Sl.	Prequalification Criteria	Supporting Documents	Doc. Provided (Y/N)
	<p>01 of the should be successful live and currently supported in Central Govt./PSU with Completion certificate within last 05 years. Should have MAF for IT infrastructure for current ICG scope</p> <p>(c) Should have implemented Secure Chat application and atleast 01 of project the should be successful live and currently supported.</p> <p>2. Reference clients should authenticate &amp; recommend the Bidder through official email within 05 days/as required by ICG, of request email sent by ICG.</p>		
(iv)	<p>The Bidder should not be blacklisted by Central/ State Government Ministry/ Department/ PSU/Government Company. Bidder also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry/Department/ PSU/ Government Company.</p>	<p>Self-declaration from the bidder in company letter head, signed by authorized signatory as per Annexure-XI</p>	
(vi)	<p>The Bidder should have ISO 9001:2008/CMMi-3</p>	<p>Valid copy of certificate at the time of bidding.</p>	
(viii)	<p>The Bidder to host and maintain web based detailed project plan in MS Project Server/equivalent including WBS, Resources assigned, Baselines, Critical Path, Stakeholders, Agile sprints, Project Milestones, Activity associated with SDLC till Go-Live and stabilization. The web based project plan should be maintained by on-site project manager/ functional expert on Payroll duly concurred by off-site project technical. A dedicated login for the Buyer should be provided from the date of signing of contract.</p>	<p>Undertaking by Bidder</p>	
(xi)	<p>Prime Bidder profile attached with Technical Bid</p>	<p>Bidder profile attached as per Appendix-'K'</p>	
(xiii)	<p>POC demo project document requirements</p>	<p>Proforma as per</p>	

Sl.	Prequalification Criteria	Supporting Documents	Doc. Provided (Y/N)
	are compiled and proforma included	Annexure-1 of Appendix-'J' attached	
(xiv)	POC of Composable IT Infrastructure	As per Appendix-'H' attached	
(xv)	Valid consortium agreement with consortium partner is included	Valid consortium agreement complying to terms & conditions of RFP is attached	
<b>Section-II: Consortium Partner/ Prime Bidder- Secure Chat application</b>			
(i)	The bidder must be incorporated and registered in India under the Indian Companies Act 1956/ LLP Act 2008 / Partnership Act 1932 and should have been operating for the last five years as on the date of publishing of Tender/ RFP notice (including name change/impact of mergers or acquisitions).	Certificate of Incorporation / Copy of Registration Certificate (s)	
(ii)	The Bidding firm must be a positive net-worth making with average annual turnover of minimum of 03 Crores company since the last three financial years: (2017 – 2018, 2016 – 2017 & 2015 – 2016)	Certificate from CA firm / P&L statement and Balance sheet approved by the auditor	
(iv)	Bidder should have atleast 01 deployment of Secure Chat application	Copy of Supply Order and Work Completion Certificates/ Demo to TEC of live deployment	
(x)	The Bidder should develop the project based on Agile methodology with clearly elaborated sprints. All customisation related code IPR shall be with ICG. The Bidder should host, maintain web based Application Lifecycle Management (ALM) software JIRA for Agile development Jira with Bit-bucket source code control, MS Project/ Oracle Primavera Project Server and provide dedicated access to ICG over internet from the date of signing of contract. The agile development plan, project plan should be concurred by on-site	Undertaking by Bidder.	

Sl.	Prequalification Criteria	Supporting Documents	Doc. Provided (Y/N)
	project manager cum on-site Payroll consultant at every stage of project development.		
(v)	The Bidder should not be blacklisted by Central/ State Government Ministry/ Department/ PSU/Government Company. Bidder also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Indian Central/ State Government Ministry/Department/ PSU/ Government Company.	Self-declaration from the bidder in company letter head, signed by authorized signatory as per Annexure-XI	
(vi)	The Bidder should have ISO 9001:2008/CMMi-3	Valid copy of certificate at the time of bidding.	
(vii)	Bidder profile attached with Technical Bid	Bidder profile attached as per Appendix-'K'	

2. **Technical Details:**

(a) **Technical Specifications:** - Design, configuration, customization, development, implementation and support for Secure Chat with Secure Application Container includes following.

(i) **Secure Chat software application:** Design, development, implementation and support for Secure Chat software

(ii) **Supply, implementation of Secure Application Container:** Supply of software licenses - 10,000 Nos. (iii) **IT infrastructure to host Secure Chat application at ICG Data Center:** Supply, deployment and support of Enterprise grade Private Cloud IT infrastructure along with necessary support

(iii) **Security Audit** by entire system including Secure Chat software and related IT infrastructure to be security audited by **CERT-IN empaneled vendor** on go-live and during warranty/ support as required by ICG

(iv) Details of Functional Requirement and Non-Functional Requirements as per **Appendix-A, Appendix-B of RFP** respectively.

(b) **Penalty clause for Service Level Agreement (SLA) violation:** -

(i) Vendor to make available online portal on 24x7 basis to raise service tickets by Buyer

(ii) Penalty clauses as per **Annexure-1 of Appendix-'A'**.

3. **Two-Bid System:** - The Prime Bidder authorised to engage consortium partner as per Bidder qualification criteria mentioned under Para-1(e) above. The case is being processed on two-bid system and, only the Technical Bid would be opened online at the time and date mentioned in Critical Date Sheet. Bidders are required to furnish clause by clause compliance of specifications bringing out clearly the deviations from specification, if any. **No price should be indicated in the Technical Bid.** Date of opening of the Commercial Bid will be intimated after Technical evaluation. Commercial Online bids of only those firms will be opened; whose Technical bids are found compliant/suitable after Technical evaluation is done by the Buyer. The following documents form part of online technical bid which should be scanned and uploaded in PDF format:-

(a) In respect of Two-bid system, Bidders are required to furnish clause by clause compliance of specifications bringing out clearly the deviations from specification, if any. The Bidders are advised to upload technical compliance statement as per Technical Bid format in **Appendix-'E'** along with Check-list as per **Appendix - 'C'** as applicable.

(b) Signed and scanned copy of Demand draft/PO in favour of the PCDA(N), Mumbai towards EMD amount or Copy of valid registration certificate regarding the firm's registration with DGS & D / NSIC / Defence Organisation (MOD) if held, for exemption of EMD. EMD to be submitted **manually** on or before bid submission end date.

(c) Self attested & scanned Copy of (i) bank details (ii) Tin No. Certificate (iii) CST Certificate (iv) VAT Certificate (v) PAN No and (vi) Certificate of acceptance of terms and conditions of RFP.

(d) Detailed breakdown of each item need to be provided as per **Annexure-1 of Appendix-'H'** format. Individual taxes need to be added as separate columns. **L1 shall be decided on overall cost of complete package consists of all bill of material and at base cost.**

(e) Bid should be uploading with covering letters as per **Appendix-'C', 'D' & 'F'** along with checklist in **Appendix-'C'**.

**Note :**

(i) **Signed & scanned copy of Technical Bids should be uploaded by Bidder under their original memo / letter pad.**

(ii) **Failure to submit any of above documents will render the bid invalid**

(iii) **Buyers reserve the right to cancel any bid without assigning any reason.**

(iv) **EMD to be submitted manually on or before bid submission end date.**

4. **Delivery Period** –The job is to be completed within **06 months** from the date of issue of job/ work order. Please note that contract can be cancelled unilaterally by the buyer in case the job is not completed within the contracted period. Extension of contracted period will be at the sole discretion of the buyer, with applicability of LD clause.

5. **INCOTERMS for Delivery and Transportation:** - CGHQ, New Delhi.

6. **Consignee details -**

Sl.	Item/ Services	Consignee
(a)	Supply of software/ hardware and delivery of associated services	<b>The Director General {for D(IT)} National Stadium Complex, New Delhi</b>

### **PART III – STANDARD CONDITIONS OF RFP**

The Bidder is required to give confirmation of their acceptance of the Standard Conditions of the Request for Proposal mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder (i.e. Seller in the Contract) as selected by the Buyer. Failure to do so may result in rejection of the Bid submitted by the Bidder.

1. **Law:** The Contract shall be considered and made in accordance with the laws of the Republic of India. The contract shall be governed by and interpreted in accordance with the laws of the Republic of India.

2. **Effective Date of the Contract:** The contract shall come into effect on the date of signatures of both the parties on the contract (Effective Date) and shall remain valid until the completion of the obligations of the parties under the contract. The deliveries and supplies and performance of the services shall commence from the effective date of the contract.

3. **Arbitration:** All disputes or differences arising out of or in connection with the contract shall be settled by bilateral discussions. Any dispute, disagreement or question arising out of or relating to the contract or relating to construction or performance, which cannot be settled amicably, may be resolved through arbitration. The standard clause of arbitration is as per Forms DPM-7, DPM-8 and DPM-9.

4. **Penalty for use of Undue influence:** The seller undertakes that he has not given, offered or promised to give, directly or indirectly, any gift, consideration, reward, commission, fees, brokerage or inducement to any person in service of the buyer or otherwise in procuring the contracts or forbearing to do or for having done or forborne to do any act in relation to the obtaining or execution of the present contract or any other contract with the Government of India for showing or forbearing to show favour or disfavour to any person in relation to the present contract or any other contract with the Government of India. Any breach of the aforesaid undertaking by the seller or any one employed by him or acting on his behalf (whether with or without the knowledge of the seller) or the commission of any offers by the seller or anyone employed by him or acting on his behalf, as defined in chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the buyer to cancel the contract and all or any other contracts with the seller and recover from the seller the amount of any loss arising from such cancellation. A decision of the buyer or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the seller. Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the seller towards any officer/employee of the buyer or to any other person in a position to influence any officer/employee of the buyer for showing any favour in relation to this or any other contract, shall render the seller to such liability/ penalty as the buyer may deem proper, including but not limited to termination of the contract, imposition of penal damages, forfeiture of the Bank Guarantee and refund of the amounts paid by the buyer.

5. **Agents / Agency Commission:** -The Seller confirms and declares to the Buyer that the Seller is the original manufacturer of the stores/provider of the services referred to in this Contract and has not engaged any individual or firm, whether Indian or foreign whatsoever, to intercede, facilitate or in any way to recommend to the

Government of India or any of its functionaries, whether officially or unofficially, to the award of the contract to the Seller; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in any way incorrect or if at a later stage it is discovered by the Buyer that the Seller has engaged any such individual/firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this contract, the Seller will be liable to refund that amount to the Buyer. The Seller will also be debarred from entering into any supply Contract with the Government of India for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract either wholly or in part, without any entitlement or compensation to the Seller who shall in such an event be liable to refund all payments made by the Buyer in terms of the Contract along with interest at the rate of 2% per annum above LIBOR rate. The Buyer will also have the right to recover any such amount from any contracts concluded earlier with the Government of India.

6. **Access to Books of Accounts:** - In case it is found to the satisfaction of the Buyer that the Seller has engaged an Agent or paid commission or influenced any person to obtain the contract as described in clauses relating to Agents/Agency Commission and penalty for use of undue influence, the Seller, on a specific request of the Buyer, shall provide necessary information/ inspection of the relevant financial documents/information.

7. **Non-disclosure of Contract documents:** - Except with the written consent of the Buyer/ Seller, other party shall not disclose the contract or any provision, specification, plan, design, pattern, sample or information thereof to any third party.

8. **Liquidated Damages:** In the event of the seller's failure to submit the Bonds, Guarantees and Documents, supply the stores/goods and conduct trials, installation of equipment, training, etc. as specified in this contract, the buyer may, at his discretion, withhold any payment until the completion of the contract. The buyer may also deduct from the seller as agreed, liquidated damages to the sum of **0.5%** of the contract price of the delayed/undelivered stores/services mentioned above for every **week** of delay or part of a week, subject to the maximum value of the Liquidated Damages being not higher than **10%** of the value of delayed stores.

9. **Termination of Contract:** The buyer shall have the right to terminate this contract in part or in full in any of the following cases: -

(a) The job is not completed for causes not attributable to Force Majeure for more than (one month) after the scheduled date of completion.

(b) The seller is declared bankrupt or becomes insolvent.

(c) The job is not completed due to causes of Force Majeure by more than (two months) provided Force Majeure clause is included in contract.

(d) The buyer has noticed that the seller has utilised the services of any Indian/Foreign agent in getting this contract and paid any commission to such individual/company etc.

(e) As per decision of the Arbitration Tribunal.

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

11. **Transfer and Sub-letting:** NA

12. **Patents and other Industrial Property Rights:** NA

13. **Amendments:** No provision of present contract shall be changed or modified in any way (including this provision) either in whole or in part except by an instrument in writing made after the date of this contract and signed on behalf of both the parties and which expressly states to amend the present contract.

14. **Taxes and Duties:**

(a) **In respect of Foreign Bidders:** - N/A

(b) **In respect of Indigenous bidders**

**(i) General**

1. If bidder desires to ask for GST or any other taxes, the same must be specifically stated. In the absence of any such stipulation, it will be presumed that the prices include all such charges and no claim for the same will be entertained.

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

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

4. If a bidder is exempted from payment of any duty/tax upto any value of supplies from them, he should clearly state that no such duty/tax will be charged by him up to the limit of exemption which he may have. If any concession is available in regard to rate/quantum of any Duty/tax, it should be brought out clearly. Stipulations like, the said duty/tax was presently not applicable but the same will be charged if it becomes leviable later on, will not be accepted unless in such cases it is clearly stated by a bidder that such duty/tax will not be charged by him even if the same becomes applicable later on. In respect of the Bidders, who fail to comply with this requirement, their quoted prices shall be loaded with the quantum of such duty/tax which is normally applicable on the item in question for the purpose of comparing their prices with other Bidders.

5. Any change in any duty/tax upward/downward as a result of any statutory variation in excise taking place within contract terms shall be allowed to the extent of actual quantum of such duty/tax paid by the supplier. Similarly, in case of downward revision in any duty/tax, the actual quantum of reduction of such



duty/tax shall be reimbursed to the buyer by the seller. All such adjustments shall include all reliefs, exemptions, rebates, concession etc. if any obtained by the seller.

**(ii) Customs Duty:** - As applicable

**(iii) Excise Duty:** -

1. Where the excise duty is payable on advalorem basis, the Bidder should submit along with the tender, the relevant form and the Manufacturer's price list showing the actual assessable value of the stores as approved by the Excise authorities.

2. Bidders should note that in case any refund of excise duty is granted to them by Excise authorities in respect of Stores supplied under the contract, they will pass on the credit to the Buyer immediately along with a certificate that the credit so passed on relates to the Excise Duty, originally paid for the stores supplied under the contract. In case of their failure to do so, within 10 days of the issue of the excise duty refund orders to them by the Excise Authorities the Buyer would be empowered to deduct a sum equivalent to the amount refunded by the Excise Authorities without any further reference to them from any of their outstanding bills against the contract or any other pending Government Contract and that no disputes on this account would be raised by them.

**(iv) GST**

If it is desired by the bidder to ask for GST to be paid as extra, the same must be specifically stated. In the absence of any such stipulation in the bid, it will be presumed that the prices quoted by the bidder are inclusive of sales tax and no liability of sales tax will be developed upon the buyer.

**(v) Local Taxes/Charges :** -

In case where the Municipality or other local body insists upon payment of these duties or taxes the same should be paid by the Seller to avoid delay in supplies and possible demurrage charges. The receipt obtained for such payment should be forwarded to the Buyer without delay together with a copy of the relevant act or bylaws/ notifications of the Municipality of the local body concerned to enable him to take up the question of refund with the concerned bodies if admissible under the said acts or rules.

15. **Pre-Integrity Pact Clause:** - N/A

**PART IV – SPECIAL CONDITIONS OF RFP**

The Bidder is required to give confirmation of their acceptance of Special Conditions of the RFP mentioned below which will automatically be considered as part of the Contract concluded with the successful Bidder (i.e. Seller in the Contract) as selected by the Buyer. Failure to do so may result in rejection of Bid submitted by the Bidder.

**1. Performance Guarantee:**

(a) **Indigenous cases:** The bidder will be required to furnish a Performance Guarantee by way of Bank Guarantee through a public sector bank or a private sector bank authorized to conduct government business (ICICI Bank Ltd., Axis Bank Ltd or HDFC Bank Ltd.) for a sum equal to **10%** of the contract value within 30 days of receipt of the confirmed order. Performance Bank Guarantee should be valid up to 60 days beyond the date of warranty. The specimen of PBG is given in Form DPM-15 (Available in MoD website).

**2. Option Clause:** - The contract will have an Option Clause, wherein the Buyer can exercise an option to procure an additional 50% of the original contracted quantity in accordance with the same terms & conditions of the present contract. This will be applicable within the currency of contract. The Bidder is to confirm the acceptance of the same for inclusion in the contract. It will be entirely the discretion of the Buyer to exercise this option or not.

**3. Repeat Order Clause** – The contract will have a Repeat Order Clause, wherein the Buyer can order upto 50% quantity of the items under the present contract within six months from the date of supply/successful completion of this contract, the cost, terms & conditions remaining the same. The Bidder is to confirm acceptance of this clause. It will be entirely the discretion of the Buyer to place the Repeat order or not.

**4. Tolerance Clause** – To take care of any change in the requirement during the period starting from issue of RFP till placement of the contract, Buyer reserves the right to 100% plus/minus increase or decrease the quantity of the required goods upto that limit without any change in the terms & conditions and prices quoted by the Seller. While awarding the contract, the quantity ordered can be increased or decreased by the Buyer within this tolerance limit.

**5. Payment Terms** - It will be mandatory for the Bidders to indicate their bank account numbers and other relevant e-payment details so that payments could be made through ECS/EFT mechanism instead of payment through cheques, wherever feasible. A copy of the model mandate form prescribed by RBI to be submitted by Bidders for receiving payments through ECS is at Form DPM-11 (Available in MoD website). The stage wise payment will be made as per the following terms and production of the requisite documents:

(a) **One-time payments-1/4** towards Design, development and implementation of Secure Chat software application(**Para-1(A) Secure Chat Development**)

SL	% of payment (Para-1(A) of Appendix-G of RFP)	Duration
(i)	10% cost (Delivery	(a) After completion of system requirement

SL	% of payment (Para-1(A) of Appendix-G of RFP)	Duration
T1	time: T0* +01 Month)	study (SRS) and acceptance by ICG.  (b) Vendor submission of Design artefacts as per UML standards, detailed project timeline in Oracle Primavera/MS Project, As Is/To Be artefact, Use Cases, Wireframes, User Acceptance Test (UAT), Product Backlog as per Agile Scrum, Sprint Backlogs, test plan, ICG login on software project ticketing & monitoring portal of Jira, Oracle Primavera/MS Project hosted and acceptance by ICG.  (c) On submission of PBG
(ii) T2	<b>Phase-I:</b> 20% cost (Delivery time: T1+01 Months)	On delivery of following: -  (a) On completion and delivery of Sprint-1 as per <b>Para-5(a) of Appendix-'A' of RFP</b>  (b) Positioning of onsite support manpower  (c) Activation of online support ticketing system
(iii) T3	<b>Phase-II:</b> 30% cost (Delivery time: T2+01 Months)	On completion and delivery of Sprint-1 as per <b>Para-5(a) of Appendix-'A' of RFP</b>
(vi) T4	<b>Phase-III:</b> Remaining 40% (Delivery time: T3+03 Months)	After 01 months of successful implementation including availability of ITSM/ALM/Project Management portal, completion of training, submission of source code, manuals, documents as per <b>Appendix-B</b> etc.

Note. \* - Date of work order is considered as 'T0'

(b) **One-time payments-2/4** towards Supply, implementation of Secure Unified Endpoint Management Software {**Para-1(B) of Appendix-G of RFP** of Secured Unified Endpoint Management Software respectively}

SL	% of payment (Para-1(B) of Appendix-G of RFP)	Duration
(i) T1	20% cost	(a) On delivery of items subject to delivery of SRS of software as per Para-5(a)(i) above. (b) Delivery of 10% (ie 1000 User licenses) of

SL	% of payment (Para-1(B) of Appendix-G of RFP)	Duration
		software licenses and successful implementation
(ii) T2	70% cost	Delivery of remaining 90% (ie 9000 User licenses) of software licenses and successful implementation
(iii) T3	10% cost	On successful final go-live of project and commencement of 01 year warranty of project

Note. \* - Date of work order is considered as 'T0'

(c) **One-time payments-3/4** towards Supply, implementation of IT infrastructure{**Para-1(C) of Appendix-G of RFP**of Secured Unified Endpoint Management Software and IT Infrastructure respectively}

SL	% of payment (Para-1(C) of Appendix-H of RFP)	Duration
(i) T1	90% cost	On delivery of items/ services subject to delivery of SRS of software as per Para-5(a)(i) above.
(ii) T2	10% cost	On successful final go-live of project and commencement of 01-year warranty of project

Note. \* - Date of work order is considered as 'T0'

(d) **One-time payments-4/4** towards Installation, support & maintenance (**Para-1(D) Installation, support & maintenance**)

SL	% of payment (Para-1(D) of Appendix-G of RFP)	Duration
(i) T1	90% cost	On delivery of items subject to delivery of SRS of software as per Para-5(a)(i) above.
(ii) T2	10% cost	On successful final go-live of project and commencement of 01 year warranty of project

(e) **Recurring payments:** -For commercial bid line items (**Para-1(E) of Appendix-G of RFP**). On completion of every 03 months after commencement of AMC. AMC to commence on completion of 01-year warranty support.

6. **Payment terms for Foreign Sellers:** - NA

7. **Advance Payments:** No advance payment(s) will be made. Stage wise payment as per para 5 above.

8. **Paying Authority:** CDA(CG), New Delhi.

(a) Indigenous Sellers: (Name and address, contact details). The payment of bills will be made on submission of the following documents by the Seller to the Paying Authority along with the bill:

- (i) Ink-signed copy of contingent bill / Seller's bill.
- (ii) Ink-signed copy of Commercial invoice / Seller's bill.
- (iii) Copy of Supply Order/Contract with U.O. number and date of IFA's concurrence, where required under delegation of powers.
- (iv) CRVs in duplicate.
- (v) Inspection note.
- (vi) Claim for statutory and other levies to be supported with requisite documents / proof of payment such as Excise duty challan, Customs duty clearance certificate, Octroi receipt, proof of payment for EPF/ESIC contribution with nominal roll of beneficiaries, etc. as applicable.
- (vii) Exemption certificate for Excise duty / Customs duty, if applicable.
- (viii) Bank guarantee for advance, if any.
- (ix) Guarantee / Warranty certificate.
- (x) Performance Bank guarantee / Indemnity bond where applicable.
- (xi) DP extension letter with CFA's sanction, U.O. number and date of IFA's concurrence, where required under delegation of powers, indicating whether extension is with or without LD.
- (xii) Details for electronic payment viz Account holder's name, Bank name, Branch name and address, Account type, Account number, IFSC code, MICR code (if these details are not incorporated in supply order/contract).
- (xiii) Any other document / certificate that may be provided for in the Supply Order / Contract.
- (xiv) User Acceptance.
- (xv) Photo copy of PBG.

9. **Fall clause** - The following fall clause will form part of the contract placed on successful bidder -

(a) The price charged for the services provided under the contract by the seller shall in no event exceed the lowest prices at which the seller provides service or offer to services of identical description to any persons/Organisation including the purchaser or any department of the Central government or any Department of state government or any statutory undertaking the central or state government as the case may be during the period till jobs as per the orders placed during the currency of the rate contract is completed.

(b) If at any time, during the said period the service provider, provides service to any person/organisation including the buyer or any Department of central Govt. or any Department of the State Government or any Statutory

undertaking of the Central or state Government as the case may be at a price lower than the price chargeable under the contract, the shall forthwith notify such reduction in service provided to the Director general of Supplies & Disposals and the price payable under the contract for the services of such reduction of service shall stand correspondingly reduced.

(c) The seller shall furnish the following certificate to the Paying Authority along with each bill for payment for supplies made against the Rate contract –  
“We certify that there has been no reduction in services charged to the Government under the contract herein and such services have not been offered/sold by me/us to any person/organisation including the purchaser or any department of Central Government or any Department of a state Government or any Statutory Undertaking of the Central or state Government as the case may be upto the date of bill/the date of completion of job against all orders placed during the currency of the Rate Contract at price lower than the price charged to the government under the contract.

10. **Exchange Rate Variation Clause:** - NA

11. **Risk & Expense clause:** -

(a) Should the software / media stores or any installment thereof not be delivered within the time or times specified in the contract documents, or if defective delivery is made in respect of the stores or any installment thereof, the Buyer shall after granting the Seller 45 days to cure the breach, be at liberty, without prejudice to the right to recover liquidated damages as a remedy for breach of contract, to declare the contract as cancelled either wholly or to the extent of such default.

(b) Should the software/media or any installment thereof not perform in accordance with the specifications / parameters provided by the SELLER during the check proof tests to be done in the BUYER's country, the BUYER shall be at liberty, without prejudice to any other remedies for breach of contract, to cancel the contract wholly or to the extent of such default.

(c) In case of a material breach that was not remedied within 45 days, the BUYER shall, having given the right of first refusal to the SELLER be at liberty to purchase, manufacture, or procure from any other source as he thinks fit, other stores of the same or similar description to make good: -

(i) Such default.

(ii) In the event of the contract being wholly determined the balance of the stores remaining to be delivered thereunder.

(d) Any excess of the purchase price, cost of manufacturer, or value of any stores procured from any other supplier as the case may be, over the contract price appropriate to such default or balance shall be recoverable from the SELLER. Such recoveries shall not exceed 2% of the value of the contract.”.

12. **Force Majeure clause:**

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

(b) In such circumstances the time stipulated for the performance of an obligation under the present contract is extended correspondingly for the period of time of action of these circumstances and their consequences.

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

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

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

13. **Buy-Back offer:** - NA

14. **Specification:** - The following specification clause will form part of the contract placed on successful Bidder –

(a) The Seller guarantees to meet the specifications as per Part-II of RFP and to incorporate the modifications to the existing design configuration to meet the specific requirement of the Buyer Services as per modifications/requirements recommended after the Maintenance Evaluation Trials. All technical literature and user manuals shall be amended as the modifications by the Seller before supply to the Buyer. The Seller, in consultation with the Buyer, may carry out technical upgradation/alterations in the design, technical literature/user manuals and specifications due to change in manufacturing procedures, indigenization or obsolescence. This will, however, not in any way, adversely affect the end specifications of the equipment. Changes in technical details, repair and maintenance techniques along with necessary tools as a result of upgradation/alterations will be provided to the Buyer free of cost within (30) days of affecting such upgradation/alterations.

15. **OEM Certificate:** - Coast Guard specific MAF certificate to be obtained from OEM and submitted as part of technical bid.

16. **Export License:** - NA
17. **Earliest Acceptable Year of Manufacture:** - NA
18. **Buyer Furnished Equipment:** - NA
19. **Transportation:** NA
20. **Air lift:** - NA
21. **Packing and Marking:** - NA
22. **Quality:** The quality of the software with media provided according to the present Contract shall correspond to the technical conditions and standards valid for the deliveries of the same services for in seller's country or specifications enumerated as per RFP and shall also include therein modification to the services suggested by the buyer. Such modifications will be mutually agreed to. The seller confirms that the services to be provided under this Contract shall be latest and shall incorporate all the latest improvements and modifications thereto.
23. **Quality Assurance:** - N/A.
24. **Inspection Authority:** The inspection will be carried out by Directorate of Information Technology on completion of the job. The mode of inspection will be departmental inspection
25. **Pre-Dispatch Inspection:** - NA
26. **Joint Receipt Inspection:** - NA
27. **Franking clause:** - NA
28. **Claims:** - NA
29. **Warranty:-**The following Warranty will form part of the contract placed on the successful bidder:-
  - (a) Except as otherwise provided in the invitation tender, the seller hereby declares that the goods, stores articles sold/supplied / services provided to the Buyer under this contract shall be of the best quality and workmanship and new in all respects and shall be strictly in accordance with the specification and particulars contained/mentioned in contract. The seller hereby guarantees that the said services (including fixing of bugs) would continue to conform to the description and quality aforesaid for a period of **36 months**/ as mentioned against individual line items from the date of provisioning of the said services to the buyer and notwithstanding the fact that the buyer may have inspected and/or approved the said services, if during the aforesaid period of 36/15 months / as mentioned against individual line items of the goods, stores articles sold/supplied are discovered not to conform to the description and quality aforesaid not giving satisfactory performance or have deteriorated, and the decision of the buyer in that behalf shall be final and binding on the seller and the buyer shall be entitled to call upon the seller to provide the entire services or such portion thereof as is found to be defective by the buyer within a reasonable period, or such specified period as may be allowed by the buyer in his discretion on application made thereof by the seller, and in such an event, the above period shall apply to the services provided from the date of rectification mentioned in warranty thereof, otherwise the seller shall pay to the buyer such compensation as may arise by reason of the breach of the warranty therein contained.



(b) The seller warrants that the goods/software supplied/installed under the contract conform to technical specifications prescribed and shall perform according to the said technical specifications.

(c) The seller warrants for a period of 36 months from the date of installation and commissioning, that the goods/stores/ software developed and installed/ supplied under the contract and each component used in the manufacture thereof shall be free from all types of defects/failures.

(d) If within the period of warranty, the goods are reported by the buyer to have failed to perform as per the specifications, the seller shall either replace or rectify the same free of charge, within a maximum period of 45 days of notification of such defect received by the seller, provided that the goods are used and maintained by the buyer as per instructions contained in the Operating Manual.

(e) The seller shall associate technical personnel of the Maintenance agency and Quality Assurance Agency of the buyer during warranty repair and shall also provide the details of complete defects, reasons and remedial actions for defects.

30. **Product Support:** - The following product support clause will form part of the contract placed on successful Bidder –

(a) The Seller agrees to provide Product Support for the software, subcontracted from other agencies/ manufacturer by the Seller for a period of **03year** after the delivery and commissioning of software application as part of software supply.

(b) In the event of any obsolescence during the above mentioned period of product support in respect of any component/ sub-system/ software, it is the liability of the seller to provide the alternate in free of cost.

(c) Any improvement/modification/ up gradation being undertaken by the Seller or their sub suppliers on the software being purchased under the Contract will be communicated by the Seller to the Buyer and, if required by the Buyer, these will be carried out by the Seller at Buyer's cost.

31. **Annual Maintenance Contract (AMC) Clause:**-The following AMC clause will form part of the contract placed on successful Bidder -

(a) The Prime Bidder through respective Consortium Vendor would provide All-Inclusive AMC (AIAMC) for a period of 2 years from the date of completion of 01 year Warranty period. AIAMC services should cover the repair and maintenance of all the equipment and systems purchased under the present Contract. The Buyer Furnished Equipment which is not covered under the purview of the AMC should be separately listed by the Seller. The seller would provide All Inclusive Annual Maintenance Contract, ITIL based service desk, ATS and renewal of licenses, required upgradation/renewal for 02 years w.e.f date of completion of 01 year warranty. Only Prime member is authorized to provide Annual Technical Support (ATS) of licenses and Web based ITIL Compliant Service Desk support. Only authorized consortium members should provide

services as directed by Centralized Service Desk and responsibilities of support area by each consortium member during installation and subsequent support period should be provided as part of Technical Offer.

32. **Engineering Support Package (ESP) clause:** - NA

33. **Price Variation (PV) Clause:** - NA

34. **Service Desk Support:** Complete technical support shall be provided by the Seller for Three Years from the date of acceptance or from date of installation and commissioning, whichever is later. The service includes spares for hardware and updates for Software would be required to maintain the equipment during its exploitation for a period of three years. The details of technical support must be submitted separately by firm with technical aspects being included in the technical offer and commercial aspects being included in the commercial offer.

35. **In Service/ Shelf Life.** The In-Service Life of the equipment shall be minimum 5 years from the date of acceptance of the offer.

36. **Prime Bidder criteria.** The invitation for bids is open to all entities registered in India who fulfill prequalification criteria as specified below:-

(a) Indian Coast Guard (Ministry of Defence, Government of India) reserves its right to subject the bidders to security clearances as it deems necessary

(b) The participation is restricted to companies registered in India

(c) The Prime Bidder of vendor consortium should provide atleast 02 item/ services out of total 03 as mentioned in para-1(A), 1(B) & 1(C) of Appendix-H of RFP on commercial bid format)

(d) Prime bidder of consortium has Office/Branch at Delhi NCR.

43. **Consortium.** It is permissible for more than one company which joins with other companies of complementing skills to undertake the scope of work defined in this RFP. It is mandatory for all consortium members to have atleast ISO 9001 certification, mandatory to have authorized for this project by respective OEM, should fulfil all particular requirements specified in the RFP in respective descriptions and having required strength of OEM certified skilled technicians at their disposal. Memorandum of Understanding (MoU)/agreement among the members signed by the Authorized Signatories of the companies to be submitted by successful vendor. The MoU /agreement shall clearly specify the Prime Bidder, stake of each member and outline the roles and responsibilities of each member. The consortium members for a particular skill area should be authorized by respective OEM, and certificate shall be submitted as part of Technical Proposal. A consortium of companies duly backed up by an Agreement/ Letter of Undertaking (to be submitted along with Technical bid) is also eligible to participate subject to the following two conditions and satisfaction of the

Tender Evaluation Committee during the evaluation of the tender. In the event of consortium being unacceptable to Coast Guard, the Prime Bidder may be given an option of going on its own.

(a) The bidder (the prime bidder in case of consortium i.e.; one of the member of the consortium that is nominated as the prime bidder by all the other members of the consortium) of this consortium shall be liable for adherence to all provisions of this Agreement.

(b) The consortium will draw upon human, technical and other resources of all the members during implementation and maintenance of the project. The Technical Bid shall include exact details in this regard, so that a consortium is not artificially created only to improve the score in Technical Bid.

(c) ATS/Service Desk- Only Prime member is authorized to provide Annual Technical Support (ATS) and Web based ITIL Compliant Service Desk support. Only authorized consortium members should provide services as directed by Centralized Service Desk and responsibilities of support area by each consortium member during installation and subsequent support period should be provided as part of Technical Offer.

## **PART V – EVALUATION CRITERIA & PRICE BID ISSUES**

1. **Evaluation and Acceptance Process.** The broad guidelines for evaluation of Bids will be as follows:

(a) Only those Bids will be evaluated on QCBS method (**Appendix-'J'**) qualifying pre-qualification criteria as per Part-II of RFP.

(b) The technical Bids forwarded by the Bidders will be evaluated by the Buyer with reference to the technical characteristics of the equipment/item as mentioned in the RFP. The compliance of Technical Bids would be determined on the basis of the parameters specified in the RFP. The Price Bids of only those Bidders will be opened whose Technical Bids would clear the technical evaluation.

(c) The Lowest Bid will be decided upon the QCBS as derived from quote by the particular Bidder as per the Price Format given in the RFP. The consideration of taxes and duties in evaluation process will be as follows:

(i) In cases where only indigenous Bidders are competing, all taxes and duties (including those for which exemption certificates are issued) quoted by the Bidders will be considered. The ultimate cost to the Buyer would be the deciding factor for ranking of Bids.

(ii) In cases where both foreign and indigenous Bidders are competing, following criteria would be followed –

(aa) In case of foreign Bidders, the basic cost (CIF) quoted by them would be the basis for the purpose of comparison of various tenders.

(ab) In case of indigenous Bidders, excise duty on fully formed equipment would be offloaded.

(ac) Sales tax and other local levies, i.e. Octroi, entry tax etc. would be ignored in case of indigenous Bidders.

(d) The Bidders are required to spell out the rates of Customs duty, Excise duty, VAT, Service Tax, etc. in unambiguous terms; otherwise their offers will be loaded with the maximum rates of duties and taxes for the purpose of comparison of prices. If reimbursement of Customs duty / Excise Duty / VAT is intended as extra, over the quoted prices, the Bidder must specifically say so. In the absence of any such stipulation it will be presumed that the prices quoted are firm and final and no claim on account of such duties will be entailed after the opening of tenders. If a Bidder chooses to quote a price inclusive of any duty and does not confirm inclusive of such duty so included is firm and final, he should clearly indicate the rate of such duty and quantum of excise duty included in the price. Failure to do so may result in ignoring of such offers summarily. If a Bidder is exempted from payment of Customs duty / Excise Duty / VAT duty upto any value

of supplies from them, they should clearly state that no excise duty will be charged by them up to the limit of exemption which they may have. If any concession is available in regard to rate/quantum of Customs duty/Excise Duty/VAT, it should be brought out clearly. Stipulations like, excise duty was presently not applicable but the same will be charged if it becomes leviable later on, will not be accepted unless in such cases it is clearly stated by a Bidder that excise duty will not be charged by him even if the same becomes applicable later on. In respect of the Bidders who fail to comply with this requirement, their quoted prices shall be loaded with the quantum of excise duty which is normally applicable on the item in question for the purpose of comparing their prices with other Bidders. The same logic applies to Customs duty and VAT also.

(e) In import cases, all the foreign quotes will be brought to a common denomination in Indian Rupees by adopting the exchange rate as BC Selling rate of the State Bank of India on the date of the opening of Price Bids.

(f) If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price will prevail and the total price will be corrected. If there is a discrepancy between words and figures, the amount in words will prevail for calculation of price.

(g) The Buyer reserves the right to evaluate the offers received by using Discounted Cash Flow method. In case cash flow involves more than one currency, the same will be brought to a common denomination in Indian Rupees by adopting exchange rate as BC Selling rate of the State Bank of India on the date of the opening of Price Bids.

(h) The Lowest Acceptable Bid will be considered further for placement of contract / Supply Order after complete clarification and price negotiations as decided by the Buyer. The Buyer will have the right to award contracts to different Bidders for being lowest in particular items. The Buyer also reserves the right to do Apportionment of Quantity, if it is convinced that Lowest Bidder is not in a position to supply full quantity in stipulated time

(j) The technical proposals forwarded by the Bidders will be evaluated by a Technical Evaluation Committee (TEC).

(i) The TEC will examine the extent of variations/differences, if any, in the technical characteristics of the Secure Chat Solution offered by various SIs with reference to the requirements specified in this RFP.

(ii) The SIs will also be asked to carry out the Proof of Concept (PoC) demonstration as per the details provided in the **Appendix-J**. Subsequent to issue of bid clarifications, Indian Coast Guard may issue additional PoC scripts at bid submission stage or later. The PoC will be targeted to address major Indian Coast Guard processes but in no way indicate or limit the scope of the functional requirements specifications of the project. Evaluation of the PoC demonstration will be carried out for compliance of the demonstrated performance of the Secure Chat

application and Secure Application solution vis-à-vis a few of the specific requirements of Indian Coast Guard

(iii) The Technical Offer will be evaluated by a Technical Evaluation Committee (TEC) to confirm that the SI and Secure Chat Solution being offered meet the essential parameters as elaborated at Appendix-A & B of this RFP. Thereafter, the SI shall carry out a PoC demonstration at 'No Cost No Commitment' basis of the application as a part of the technical evaluation process, as per the PoC scripts given in Appendix-J or issued later at the stage of bid submission or at any time prior to completion of TEC.

(k) Evaluation of Commercial Proposals. The commercial proposals of the SIs whose offer is short-listed, after technical trials and evaluation have been accepted technically will only be opened and a comparative statement will be prepared. Comparison of offers will also be done on the same basis. The SI quoting lowest price (L1) based on QCBS evaluation as determined by Contracts Negotiation Committee (CNC), would be invited for negotiations by CNC. Details of Technical/ Commercial Evaluation of proposals as per **Appendix-'E'**.

(l) The Bidders are required to spell out the rates of Customs duty, Excise duty, VAT, Service Tax, etc. in unambiguous terms; otherwise their offers will be loaded with the maximum rates of duties and taxes for the purpose of comparison of prices. If reimbursement of Customs duty / Excise Duty / VAT is intended as extra, over the quoted prices, the Bidder must specifically say so. In the absence of any such stipulation it will be presumed that the prices quoted are firm and final and no claim on account of such duties will be entailed after the opening of tenders. If a Bidder chooses to quote a price inclusive of any duty and does not confirm inclusive of such duty so included is firm and final, he should clearly indicate the rate of such duty and quantum of excise duty included in the price. Failure to do so may result in ignoring of such offers summarily. If a Bidder is exempted from payment of Customs duty / Excise Duty / VAT duty upto any value of supplies from them, they should clearly state that no excise duty will be charged by them up to the limit of exemption which they may have. If any concession is available in regard to rate/quantum of Customs duty / Excise Duty / VAT, it should be brought out clearly. Stipulations like, excise duty was presently not applicable but the same will be charged if it becomes leviable later on, will not be accepted unless in such cases it is clearly stated by a Bidder that excise duty will not be charged by him even if the same becomes applicable later on. In respect of the Bidders who fail to comply with this requirement, their quoted prices shall be loaded with the quantum of excise duty which is normally applicable on the item in question for the purpose of comparing their prices with other Bidders. The same logic applies to Customs duty and VAT also.

(m) If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price will prevail

and the total price will be corrected. If there is a discrepancy between words and figures, the amount in words will prevail for calculation of price.

2. **Price bid format**: As per **Appendix-'H'** of RFP.
3. The bidders are required to **UPLOAD** following:
  - (a) The Commercial bid format is provided as **BoQ.xls** along with this tender document at **<https://eprocure.gov.in>**. Bidders are advised **to download this BoQ.xls** as it is and quote their offer in the permitted column. **Bidders are also to fill the duties & Taxes columns as applicable**
  - (b) The Price Bid Format as per **Appendix-'H'** as required. Determination of L-1 will be done based on total of basic prices (**not including** levies, taxes and duties levied by Central/State/Local governments such as excise duty, VAT, Service tax, Octroi/entry tax, etc. on final product) of all items/requirements as mentioned above.

**Appendix-'A'**

*(Refer to Para-2(a)(i),(ii),(iii) of Part-II of RFP  
, Para-5(b) of Part-IV of RFP)*

**TECHNICAL REQUIREMENTS - DESIGN, DEVELOPMENT, IMPLEMENTATION  
AND SUPPORT FOR SECURE CHAT WITH SECURE APPLICATION CONTAINER  
(PROJECT TAPPS) - INDIAN COAST GUARD**

**Background.**

1. Indian Coast Guard (ICG) is the fourth armed force of Indian Union and is mandated to take actions as deemed fit to protect India's maritime and other national interests in the maritime zones of India. ICG carry out surveillance of 7,500 kms long coastline, 2.02 million Sq. Km of Exclusive Economic Zone (EEZ) and over 06 million SqKms of Indian Maritime Search & Rescue Region (ISRR) to enforce Indian and International maritime laws and to provide swift Search and Rescue (SAR) support across ISSR using conventional assets such as ships and aircraft.
2. ICG as part of ongoing digitization efforts intend to implement a software application to enable ICG personnel collaborate through secure chat messenger with enhanced security on turn-key basis.

**OBJECTIVE**

3. Objective of ICG Secure Chat with Secure application container is to provide safe & secure ICG specific messenger application for all ICG personnel and manage all ICG mobile applications in secure environment. The Bidder should include required features to achieve objectives during SRS stage of project and discrepancies if any, the decision of the Buyer is final and has binding on the Bidder.
  - (a) Design, develop, implement Secure chat software. Secure Chat to provide following key features for ICG Personnel.
    - (i) One-to-One secure text messages, voice, video calls
    - (ii) One-to-Group broadcast secure messages
    - (iii) Messages over SMS carrier in case of lack of internet coverage
    - (iv) Secure all photos, documents shared over Secure Chat
    - (v) Maintain privacy of ICG Personnel by restricting security to ICG mobile application container only
    - (vi) Integrate with ICG software applications such as HR applications (HIIMIS/EPMIS), Payroll application (PARAM), CGBA applications, Healthcare application (ASHA) etc.



(vii) Securely host/ manage with ICG mobile/ desktop software applications such as HR applications (HIIMIS/EPMIS), Payroll application (PARAM), CGBA applications, Healthcare application (ASHA) and integrated ICG Mobile application (MITRA) etc.

(viii) Provide integrated highly secured environment for all ICG Personnel/ Unit applications over internet, distributed over Bring Your Own Device (BYOD) environment which includes personnel mobile phones/tab of Android/ iOS, laptop/ desktop of MS Windows/ Apple Mac books

### **SCOPE OF WORK**

4. Vendor should Design, development, implementation and support for Secure Chat with Secure application container and required hardware/ software on **turnkey basis**. Secure chat application should be designed, developed on J2EE platform for Web based Management console and native Android/ iOS for Chat client application to achieve as mentioned in **Appendix- 'B'** to achieve seamless integration of data, maintenance, licensing optimization etc. The Bidder should include required features to achieve following objectives during SRS stage of project and discrepancies if any, the decision of the Buyer is final and has binding on the Bidder. Detailed functional requirements are detailed in succeeding paragraphs.

5. **Design, develop, implement Secure chat software.** Secure Chat to provide following key features for ICG Personnel.

(a) Sprint-1 deliverables

- (i) One-to-One secure text messages
- (ii) One-to-Group broadcast secure messages
- (iii) Send/ Receive documents/ multimedia contents and store securely with Unified Endpoint Management Software (UEM)
- (iv) Integration with UEM for application management
- (v) Single-Sign-On

(b) Sprint-2 deliverables

- (i) One-to-One secure voice, video calls
- (ii) Messages over SMS carrier in case of lack of internet coverage
- (iii) Integrate with ICG application to send/ receive text messages over RESTful API

(c) Sprint-3 Should deliver rest of the requirements as per RFP

(e) Integrate with ICG software applications such as HR applications (HIIMIS/EPMIS), Payroll application (PARAM), CGBA applications, Healthcare application (ASHA) etc.

(f) Maintain privacy of ICG Personnel by restricting security to ICG mobile application container only

(g) Detailed sizing and technical specifications as per Appendix-B and Annexure-i of Appendix-B of RFP

6. **Secure application container.** Supply, integrate and support for Secure mobile application container.

(a) Securely host/ manage with ICG mobile/ desktop software applications such as HR applications (HIIMIS/EPMIS), Payroll application (PARAM), CGBA applications, Healthcare application (ASHA) and integrated ICG Mobile application (MITRA) etc.

(b) Provide integrated highly secured environment for all ICG Personnel/ Unit applications over internet, distributed over Bring Your Own Device (BYOD) environment which includes personnel mobile phones/tab of Android/ iOS, laptop/ desktop of MS Windows/ Apple Mac books

(c) Detailed sizing technical specifications as per Appendix-B and Annexure-i of Appendix-B of RFP

7. **Secure hosting of application on ICG Private Cloud Virtualised infrastructure.**

(a) Supply, establish ICG Private Cloud Virtualised infrastructure environment for deployment of Secure Chat application and Secure Container software

(b) Provide Composable IT infrastructure hardware to natively achieve multi-hypervisor, bare metal, container supported private cloud environment

(c) Supply, integrate required hardware including Tape Library, Rack Server to support D2D2T Business Continuity architecture with suitable Backup/recovery/replication software

(d) Provide required Application Load Balancer (ALB) with SSL/TLS security to support Application level Virtual Private Network (VPN) for BYOD devices

(e) Design, establish Militarized Zone, De-Militarized Zone to secure software applications using virtual Next Generation Firewall (NGFW) as required

(f) Design, establish Militarized Zone, De-Militarized Zone to secure software applications using virtual Web Application Firewall (WAF) as required

(g) Detailed sizing technical specifications as per Appendix-B and Annexure-i of Appendix-B of RFP

8. **Support and penalty.** Vendor should provide 01 onsite Support Engineer well versed with functional aspects of project. Vendor should provide satisfactory support as required, failure to do, shall attract penalty clauses as enumerated in Annexure-I of Appendix-A, which is on and above other penalty clauses applicable.

9. Functional requirements are indicative in nature. Final functional requirements shall be identified as part of SRS phase by vendor.

**Note: Bidders are requested to refrain from attaching additional unwanted documents.**

## **Annexure-1**

(Refers to Appendix 'A')

### **DETAILS OF PENALTY CLAUSES**

1. Application not made fully operational within 02 working days – Rs. 2000 per day will be levied for each day of non-availability of system. In case situation exceeds 05 working days, enhanced penalty of Rs.5000 per day is applicable.
2. Late reporting to work by onsite support engineer/ manpower Rs. 500/- Per day (Support engineer/ manpower need to report for work at 0830 hrs. In a month maximum ten late reporting is permissible for entire resident engineer subject to maximum 03 late reporting).
3. In the event of support engineer/manpower remaining absent/on leave without substitute there of - Rs 1500/ for each day of absence.
4. Failure to maintain/renew/extend performance bank guarantee – Rs 1000/- per day (PBG should be restored to 100% if it is dip below 70% within 10 days. PBG should not fall below 60%. In case of AIAMC extension, PBG should be renewed for the same value irrespective viz-a-viz of period of such extension, i.e pro-rata not applicable. Coast Guard not mandated to return PBG before the expiry of initial validity period, and it is the responsibility of vendor to arrange PBG accordingly without any break in PBG availability).
5. ITSM software should be updated on daily basis and each service ticket should be assigned with unique ticket ID by onsite support engineer. Failure to update – Rs.500 per day. ITSM software shall be made available by Vendor on 24x7 basis at their premises with dedicated login for ICG to create/manage support tickets.
6. ITSM Service Desk portal and ALM portals should be available on 365x24x7 during the entire contract period with minimum availability of 99%. Non-availability of ITSM Portal for more than 24 hours – Rs.1000 per day. Mutually agreed maintenance periods and other justifiable circumstances as accepted by Coast Guard are exempted.
7. Oracle Primavera/MS Project portal to be hosted, updated and should be available on 365x24x7 during the till final GoLive + 06 months with minimum availability of 99%. Non-availability of Oracle Primavera/MS Project Portal for more than 24 hours – Rs.1000 per day. Mutually agreed maintenance periods and other justifiable circumstances as accepted by Coast Guard are exempted.
8. JIRA or equivalent Application Lifecycle Management (ALM) including source code management, bug tracking, resource scheduling portal should be available on 365x24x7 during the entire contract period with minimum availability of 99.9%. Non-availability of ALM Portal for more than 24 hours – Rs.1000 per day. Mutually agreed maintenance periods and other justifiable circumstances as accepted by Coast Guard are exempted.
9. In case the vendor is not in a position to provide alternate/standby facility, Buyer shall have the right to get the issues rectified by a third party without effecting the contractors' obligations for maintenance of the systems under the contract. The

payment towards maintenance/ repair charges will be made to the third party and a sum equal to maintenance/ repair charges would be deducted from any outstanding bills/ PBG for the time actually lost.

10. All penalty amounts may be deducted from outstanding bills/Performance Bank Guarantee as applicable.

11. It may also be noted that in case of vender backing out in mid-stream without any explicit consent of Coast Guard, the vender will be liable to recovery at higher rates vis- a- vis those contracted with, which may have to be incurred by Coast Guard on maintenance of IT system for the balance period of contract by alternative means.

12. Under no circumstances, on each occasion the cumulative continuous penalty total shall not exceed 5% of the contract value.

13. Coast Guard at its discretion may entirely/partly waive-off penalty under justifiable circumstances.

**NON-FUNCTIONAL REQUIREMENTS – PROJECT TAPPS**  
**FOR INDIAN COAST GUARD**

**TAPPS specific non-functional requirements**

**1. Software development methodology**

(a) **Agile development based on Scrum** to be deployed with clearly mentioned Sprints during SRS. Minimum of 05 sprints with initial delivery in 90 days from date of work order.

(b) Software should be developed on **Application Lifecycle Management (ALM)** and dedicated login should be provided for ICG

(c) Entire software should be developed on Service Oriented Architecture (SOA), preferably using Micro services on Container.

**2. Application middleware stack features** (*Licenses shall be provided by ICG as required*)

(a) Enterprise Portal

(d) Enterprise Service Bus (ESB) Server

(c) Document Management System (DMS)

(d) MS Active Directory/ LDAP Server based authentication

(e) Single-Sign-On

(f) Oracle Database with Golden Gate, Mobile Server, Advanced Data Encryption, Label Security and Data Vault

(l) Application Lifecycle Management Server (ALM) like JIRA

(m) Vendor should provide support for Middleware stack, preferably of RedHat JBOSS or equivalent.

**3. Inter-operability with ICG ERP/Software Systems.** Should provide Secure Chat web services API as required as per open-standards such as RESTful APIs to enable inter-operability with ICG ERP/Software systems. All required licenses should be included.

**4. User Management**

(a) **Central Admin - TAPPS** should be enabled for.

(i) Create groups based on ICG Active Directory

(ii) Default groups based on Organisational Unit (OU) of ICG Active Directory

(iii) Create custom group on any combination of OU

(iv) Delegate/ Invoke group admin to designated groups as available in ICG Active Directory

(v) Same 'Group admin' may be admin for one or more modules.

(vi) Integrate with ICG IAM for centralised Roles management

(b) **Group Admin - TAPPS** is responsible for administration of group of users belong to particular unit/ combination of units. 'Group Admin' are created and managed by 'Central Admin'. Group Admin shall have following functionalities.

- (i) Add/remove user/groups to pre-defined roles
- (ii) Assign privileges as required.

5. **Access Control List (ACL) features.**

- (a) Basic components of ACL are 'Roles' and 'Privileges'
- (b) ICG units are to be organized as 'Unit' and managed by 'Group/Unit Admin'
- (c) 'Group/Unit Admin' created and managed by 'Central Admin'. 'Central Admin' may create 'Group/Unit Admin' and assign any particular group from ICG AD for administration
- (d) ICG users are added into particular 'Group/ Unit' by respective 'Group/Unit Admin' and assigned required privileges
- (e) 'Group/ Unit Admin' shall have view of all eOffice activities related to particular unit only and shall never have access to other 'Group/ Units'. Similar to multi-tenancy feature of software systems
- (f) Workflow may span across multiple units, users
- (g) Dashboard for 'Central Admin' and 'Group/Unit Admin' should have following features.
  - (i) Should display graphical representation of entire 'Group/ Unit Admin' and assigned users/ roles with drill-down option.
  - (ii) Should display graphical charts for user vs login counts, user vs module access counts, user vs business process counts, dormant user statistics, dormant business process statistics and least/most used business process statistics
  - (iii) Detailed logs should be generated and made available for ICG SIEM software system to enable central monitoring of software usage pattern.

6. **Web portal standards**

- (a) Should be based on '**Responsive Web Design (RWD)**' and should adapt the layout to the viewing environment by using fluid, proportion-based grids, flexible images etc. RWD should be thoroughly tested before delivery of each sprint/ patches to Coast Guard
- (b) Should provide atleast Graphical User Interface (GUI) design templates for User to select as per preference
- (c) **Navigation.** Should use left navigation with cascading levels upto three with collapsible navigation panels. First level to display major modules, and TAPPS to be considered as one of the major module. On click of 'TAPPS' first level, 2<sup>nd</sup> navigation panel should provide module level menus and on-click of 2<sup>nd</sup>

Navigation menu, main content page should provide context sensitive data/ or further menu/ options as required by Coast Guard

(d) Breadcrumb to be provided at global level

(e) **Help.** Help should be provided through Tooltip, footer help display and on selection of 'F1', a right side panel should be displayed with collapsible capability. F1 help panel should toggle to collapse on press of 'F1'

(f) Bidder to provide atleast 03 themes as part of Software Requirement Specification (SRS) and **wireframe templates** for approval of Coast Guard. Bidder should proceed with development only on approval of wireframes by Coast Guard

(g) **Independent unique home page** should be provided for each ICG User, ICG Unit as required by Coast Guard. User home/ landing page should have graphical charts to display statistics within the context of particular ICG User, ICG Unit and User Designation/ Role. User should be able to 'pin' module/ functionality of his/her favorite in their 'Home' page.

7. **One database& replication.** Bidder should develop entire software stack based on MySQL/ Oracle Database as provided by Coast Guard. Bidder should use all security features of MySQL/ Oracle database such as Label security, Data Encryption and Data Vault. All data intensive queries should be implemented using Oracle PL/SQL stored procedures. All replication related functionality should be based on 'Oracle Golden Gate' functionality only and such functionalities should not be developed at application level.

8. Should be developed and deployed in Enterprise Middleware platform including **Java EE Application Server** and compatible with leading Java EE Application Servers of Oracle WebLogic/ IBM WebSphere/ RedHat JBOSS

9. TAPPS portal component shall be maintained by the vendor and shall be developed for ongoing new features by Coast Guard in-house software development team. Vendor should provide and support pre-configured JDeveloper IDE environment for development TAPPS Portal by Coast Guard.

10. **Multi-tenant, federated instance features**

(a) System should support multi-tenancy.

(b) All federated instances should be in sync with primary instance at Coast Guard Data Center at Delhi NCR

(c) Should group ICG units into logical, hierarchical for management flexibility and deploy policies centrally to be used in conjunction with regional or functional policies. Delegate appropriate levels of administrative control at the regional level or centrally with role-based management.

11. **Federated, local survivability and off-line features for Secure Chat**

(a) Designated federated installations should support local survivability to provide key features as required by ICG for Secure Chat.

12. **Support**

(a) Support for one year from the date of go-live and AMC for 02 more years/ or as mentioned in RFP.



- (b) Support to include minor feature updates, bug fixes
- (c) Support for Coast Guard in-house/ 3<sup>rd</sup> party developers for updating/ maintenance of SSO, Portal and ESB.

13. **Integration with email**, task, contacts & calendar of MS Exchange/ NIC Email Server.

14. **Project management requirements.**

- (a) Detailed project timeline should be provided with SRS
- (b) Project plan to be planned in Oracle Primavera/ Microsoft Project server hosted by Bidder and dedicated login to be provided to ICG. Project timeline & artefacts should be updated for every versions/ stages as per ICG requirement.
- (c) Project data sheet should be compatible with Oracle Primavera/ Microsoft Project Server. Vendor should submit/ upload into internal ICG project management servers as required by ICG
- (k) Skilled manpower to be assigned to project, should be available for fortnightly review/ as required by ICG. Details of project members alongwith standby members (atleast 01 for each) to be provided. **Project members should not be changed without explicit permission of ICG and violation of the same shall be treated seriously and contract may be terminated with forfeiture of bank guarantee alongwith other obligations.** Minimum composition of project management team should as be following.
  - (i) Project Manager, PMP certified (**Single-Point-of-Contact**)
  - (ii) Business Analyst
  - (iii) Senior Java Developer
  - (iv) Senior Test Engineer
  - (v) Senior Middleware Developer
  - (vi) Database Developer
  - (vii) GUI Designer
  - (viii) Document Engineer
- (l) Minute of meetings should be commented & concurred by official email by Project Manager, Certified Test-in-charge, GUI designer and Database designer. Such comments/ concurrences should be made available within 03 working days and exemption, if any with explicit approval of ICG.
- (m) ICG may resort to cancellation of work order with forfeiture of EMD/ PBG, penalty clauses as applicable and other contractual clauses as deemed fit for following situations.
  - (i) Change of project members without explicit concurrence of ICG
  - (ii) Failure to provide replacement manpower within committed timeline
  - (iii) Non-availability of project management manpower for review meeting

(iv) Not responding and not providing concurrence/ non-concurrence for 'Minutes of meeting' by project team members within ICG specified timeline

**15. Source code for Non-COTS features & customizations.**

(a) ICG shall hold Intellectual Property Rights (IPR) on source code & documentation related to all 'Non-COTS' features and customisations. In case of disagreement on designation of 'Non-COTS' features, decision of ICG shall be final.

(b) Should be in compliance to 'Software Development & Re-Engineering Guidelines for Cloud Ready Applications Version 2.1 or latest as issued by Govt. of India' and ICG specifications. Decision of ICG is final in case of different interpretations of Government of India guidelines.

(c) Software for each stages prior to Go-live/ Post Go-live should be compiled & ported to ICG central version control software

(d) Complete documentation to create initial release software & subsequent builds.

**16. IT Service Desk for support.**

(a) Vendor should provide IT Service Desk portal for ICG on receipt of work order

(b) IT Service Desk software should be in compliance with ITIL standards and the same to be explicitly highlighted on respective COTS/ FOSS product specification

**17. Service Level Agreement (SLA) requirements** as following. Non-adherence of SLA shall invite penalty as mentioned in Appendix-'C'.

(a) Software application should be made available 24x7 basis and all service tickets raised through email/service portal should be responded within 04 working hours and to be resolved within 48 hours. Any specific request for change in response time should be concurred by Buyer on case to case basis

(b) IT service desk portal should provide 24x7 ticket creation facility to Buyer. ITSM should generate automated email to Buyer given official email ID during entire lifecycle of ticket for key phases including creation, assigned, resolved, hold and closed.

(c) Onsite support engineer should report to work at 0830hrs on all working days of Coast Guard

(d) Onsite support engineer should not be changed without explicit concurrence of Buyer

(e) Any replacement to support engineer should have obtained OEM Certified resource/ Experienced as acceptable to ICG with required skillset and experience as per RFP clauses. Any delay in provision of appropriate skilled manpower shall be treated as absent of service engineer and relevant penalty clauses shall be made applicable.

## **Standard non-functional requirements**

18. **Enterprise Application Integration (EAI) requirement.** Coast Guard intend to build seamless integration between various software applications and avoid 'islands automation/ information silos'. Hence, compliance to EAI requirement of Coast Guard is one of the fundamental requirement.

- (a) Should support "**unrestricted sharing of data and business processes among any connected application or data sources in the enterprise**"
- (b) Should provide 'Data Dictionary', 'Business Process Dictionary' and detailed API interface specifications
- (c) Should support various web services API including RESTful
- (d) Should support integration with Coast Guard Primary ESB Application Integration Platform.

## 19. **Single-Sign-On (SSO) features**

- (a) Should be implemented as Central SSO for Coast Guard
- (b) SSO to use Coast Guard Active Directory as underlying Directory Services
- (c) Should have 'High-Availability (HA)' characteristics across primary & DR server rooms of Coast Guard
- (d) Should integrate with Coast Guard Security Information and Event Management (SIEM) systems

## 20. **Application Lifecycle Management (ALM) portal.**

- (a) Vendor should deploy and maintain ALM portal such as JIRA. ALM should consists of source code server on Git, document server, collaboration server for team interaction. Development of software should be on deployed ALM only.
- (b) Vendor should provide dedicated user accounts on ALM portal for Coast Guard
- (c) ALM portal should manage all Non-COTS related customizations & development. IPR shall be with ICG for all source code except COTS.
- (d) Should provide all development related documentations including wireframe, SRS, business use cases, use cases, traceability matrix, test plans, test reports, deployment plans, database ER diagrams and API specifications for EAI compliance.

## 21. **Integration with ICG IAM (Identity and Access Management) system.**

- (a) ASHA should support IAM and enable staff onboarding feature
- (b) Support IAM from leading vendors such as IBM/ Microsoft/ Dell RSA and Oracle
- (c) All roles should be exposed to IAM for centralised user management

22. **Provide API for internet website and mobile app**

- (a) Provide required RESTful API for appointment process through internet website and mobile app
- (b) Expose selected functionalities for internet and mobile app

23. **Miscellaneous non-functional requirements**

- (a) Implementation, integration of on-campus PKI infrastructure
- (b) Database backup & restore
- (c) Virtualization compatible
- (d) High Availability configuration model
- (e) Active Directory integration information
- (f) Cloud-ready features/ compatibility metrics
- (g) Integration with touch-enabled features
- (h) User Management with switch role functionality
- (j) Provide unified intranet portal which should be updated through ESB. It is required in compliance to ICG SIMHA unified architecture.

24. **Training.** Onsite training at Delhi NCR/ Chennai by qualified instructors should be provided to ICG personnel as follows.

<b>Sl</b>	<b>Training</b>	<b>Location</b>	<b>Personnel per Batch</b>
(a)	System administration, installation, backup & recovery, 01 Batch	Delhi NCR	02
(b)	User training	Delhi NCR	25

25. **Security Audit by CERT-IN empaneled vendor**

- (a) Secure Chat application should be audited before go-live
- (b) Secure Chat application should be audited whenever required during warranty & support period
- (c) Entire IT infrastructure alongwith software supporting the Secure Chat application should be audited including project warranty period as required by ICG

26. **Documentation.**

- (a) Design standards for documents:
  - (i) Software Requirement Specification (SRS) as per ISO/IEC/IEEE 29148-2011 specifications or latest

- (ii) Modeling language should be based on UML version 2.5-2015 or latest. All design documents should be clearly documented & generated in CASE tools supporting UML 2.5-2015 or later.
- (iii) Test plan should be based on IEEE 829-2008 or later.
- (b) Vendor to deliver required documents strictly within specified timeline for each stage. In case of delay, Buyer at liberty to terminate the contract.
- (b) Stage-I: Software Requirement Specification (SRS).
  - (i) SRS should be submitted within 10 days of date of Coast Guard work order. Vendor could enter into prior development initiate design & development phase only after obtaining approval of SRS
  - (ii) SRS and project planning with timeline is hosted on Oracle Primavera/ MS Project at Bidder servers and dedicated login be provided to ICG
  - (ii) Initial version of EAI specifications to be provided
  - (iii) Artefact to be delivered: SRS
  - (iv) Timeline: 10 days from on receipt of work order.
- (c) Stage-II: Prior development phase.
  - (i) Documents should be prepared as per UML standards. Vendor to provide business use cases, detailed use cases, list of actors, wireframes designs and traceability matrix.
  - (ii) Traceability matrix should clearly indicate trace between business use cases/ use cases/ wireframe/ planned version/ timeline/ associated project members/ components/ test plan and source code repository details. Traceability matrix should have 'Use Case' as primary reference column.
  - (iii) Test cases, data dictionary, terminology specific to project, logical database design, logical ER-design diagram, RESTful services API definitions, class diagram, deployment diagram during development of software.
  - (iv) Updated version of EAI specification be provided
  - (v) On approval of documents by Buyer only Vendor should officially commence development. Buyer may terminate contract in case of delay Failure to submit documents as per Buyer requirement sh
  - (vi) Artefacts to be delivered: Business use case, Use cases (fully-dressed UML format), Wireframe design, list of actors, test plan, timeline in MS Project/ Equivalent format, Bi-weekly project review meeting format, Minutes of meeting format and traceability matrix
  - (vii) Timeline: 02 months from work order date.
- (c) Stage-III: During development. Class diagrams, package diagrams, interface, RESTful service related to use cases under development, updated wireframe, source code repository details, ALM ticket details related to bug/ minor enhancement/ minor changes as applicable for current development,

regular updated test plan, updated EAI details, update ICG MediaWiki as and when required to update related diagrams and project development documents.

(d) Stage-IV: On release of each version of software. Update of ICG MediaWiki/ ICG DMS document repository with all related documents, interactive multimedia video contents.

(e) Stage-V: On Go Live. Vendor to provide design & developments artefacts as mentioned in Form-1 as per enclosure.

(f) Interactive web documentation/ manual/ training. Buyer has deployed 'DMS as part of SIMHA platform' as standard documentation/ training knowledge repository as on-campus deployment inside militarised zone with no access over internet to Vendor. Vendor should provide standard visual training/ deployment/ technical as per ICG standards preferably developed on Adobe Premiere/Equivalent. ICG DMS shall be made available to vendor at ICG campus. Vendor has to customise/ update as required to provide complete end-to-end maintenance/training material which should include step-by-step installation of application under development, project design documents such as wireframe/ details of project members/ use case diagrams/ project timeline/ screenshots of important setup/ configurations, maintenance steps, backup & recovery steps and detailed feature demonstrations.

### **IT Hardware specific non-functional requirements**

27. Technical requirements for each of major components should be as per '**Annexure-I of Appendix-B**'.

28. **Single-pane-of-glass-monitoring.** IT hardware units to be deployed at Data Center and Disaster Recovery Data Centers. Entire system should be centrally manageable, deployable through 'Single-glass-pane-monitoring' software console. All IT hardware/ software components such as hardware servers should have native 'Single-pane-of-glass-monitoring' to display all necessary parameters in single unified Dashboard as mentioned in '**Annexure-I of Appendix-B**'.

**Annexure-I of Appendix-'B'**

**DETAILED TECHNICAL SPECIFICATIONS -  
ENTERPRISE SECURE CHAT, UNIFIED ENDPOINT MANAGEMENT WITH HIGH-  
AVAILABILITY IT INFRASTRUCTURE**

Table of Contents

Part-I: ITInfrastructure Minimum Required Sizing

Part-II: IT Infrastructure - Detailed Technical Specifications

**PART-I: SECURE CHAT WITH UNIFIED ENDPOINT MANAGEMENT SYSTEM IT  
INFRASTRUCTURE MINIMUM REQUIRED SIZING**

<b>Sl.</b>	<b>IT Infrastructure Type</b>	<b>Sizing</b>	<b>Detailed Specifications</b>	<b>Complied (Yes/ No)</b>
1.	Enterprise Secure Chat Software	(a) Intellectual Property Rights (IPR) with Coast Guard (b) Qty.-01 No.	Section-A of Annexure-1/ Appendix-B	
2.	Unified Endpoint Management Software	(a) Qty.-10,000 Nos. (b) 03 Years warranty with OEM support	Section-B of Annexure-1/ Appendix-B	
3.	Composable IT Infrastructure with SDDC capabilities	(a) Chassis: 01 No. (b) Compute Node/ Chassis, 2x20 Cores, 512GB RAM, 2TB SSD in RAID-10: Qty.- 02 Nos. (c) Storage Nodes/ Chassis, 10TB in RAID-10, NL-SAS: Qty.-01 No.	Section-C of Annexure-1/ Appendix-B	
4.	Tape Library	(a) Qty.-01 No. (b) Tape qty.-12 Nos. of each LTO-7, 6TB each	Section-D of Annexure-1/ Appendix-B	
5.	Rack Server	(a) Qty.-02 No. (b) CPU -01 x 14 Core, 2.4Ghz	Section-E of Annexure-1/ Appendix-B	
6.	SAN Switch	Qty.- 02 No.	Section-F of Annexure-1/ Appendix-B	
7.	Virtual Next Generation Firewall with WAF	(a) Throughput-05 Gbps (b) Qty. 02 Nos. in HA/ Active-Active	Section-G of Annexure-1/ Appendix-B	

<b>Sl.</b>	<b>IT Infrastructure Type</b>	<b>Sizing</b>	<b>Detailed Specifications</b>	<b>Complied (Yes/ No)</b>
8.	Private Cloud Virtualisation Software	Qty.-04 CPU	Section-H of Annexure-1/ Appendix-B	
9.	Backup Software	Qty.-04 CPU	Section-J of Annexure-1/ Appendix-B	
10.	OEM Qualification, Warranty & Implementation support	Warranty 03 Years from GoLive	Section-K of Annexure-1/ Appendix-B	



**PART-II: SECURE CHAT WITH UNIFIED ENDPOINT MANAGEMENT SYSTEM IT INFRASTRUCTURE – DETAILED SPECIFICATIONS**

**Index of Sections**

<b>Sl.</b>	<b>Section</b>	<b>Description</b>	<b>Complied (Yes/ No)</b>
1.	Section-A	Enterprise Secure Chat Software	
2.	Section-B	Unified Endpoint Management Software	
3.	Section-C	Composable IT Infrastructure	
4.	Section-D	Tape Library	
5.	Section-E	Rack Server	
6.	Section-F	SAN Switch	
7.	Section-G	Virtual NGFW with WAF	
8.	Section-H	Private Cloud Virtualisation Software	
9.	Section-J	Backup, recovery and replication software	
10.	Section-K	OEM Qualification, Warranty & Implementation Support	

Section-A – **Enterprise Secure Chat Software**

<b>Sl.</b>	<b>Category</b>	<b>Technical Requirements - Secure Chat</b>	<b>Complied (Yes/ No)</b>
1.0	<b>Deployment</b>	<p><u>On-premise Hosting</u></p> <p>(a) Shall be hosted on-premises, end-to-end controlled and managed by Indian Coast Guard (ICG) with no 3rd party access to data</p> <p>(b) Shall support private cloud environment based on vSphere, Hyper-V and KVM</p> <p>(c) Shall support load balancing, high-availability architecture</p> <p>(d) Provision is made so that client app can be hosted on the ICG enterprise store instead of play store or app store. Shall support leading Enterprise Mobility Management (EMM)s including VMware, IBM, Citrix</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
1.1		<p><u>ServerComponents</u></p> <p>(a) Server for Chat Web Console for System Configuration, interact for user management of the enterprises for fetching employee information. Interact with Chat Server for managing chat users and groups and defining the rules and policies for the group chat</p> <p>(b) Chat Server is an OpenFire/equivalent server component for messages handing - storage of messages on the Chat Server for sharing within the users and chat groups And file transfer handling to handle file transfer of different types of files like Audio, Video, Images, PDF Docs, etc. Files will be maintained on the server for definite period for sharing across users</p> <p>(c) Key Management Store (KMS) to manage the key store for encrypted messages and contents and manage private and public keys</p> <p>(d) Relational Database (RDBMS) for server data for the above components. Shall support Oracle and MySQL</p>	
1.2		<p><u>Data Integrity</u></p> <p>(a) Shall provide suitable mechanism to ensure User data integrity in Servers/ Client locations</p> <p>(b) Shall provide adequate protection against access to User data by unauthorised systems/ personnel</p> <p>(c) Shall provide audit logs</p>	
1.3		<p><u>Certification</u></p> <p>(a) Chat app must be STQC certified for security, performance and documentation and comply to coding standards as per Govt. of Indian guidelines</p> <p>(b) Components of the apps to be certified are as following: -</p> <ul style="list-style-type: none"> <li>(i) Secured Chat Server Web Console</li> <li>(ii) Secured Chat Android App</li> <li>(iii) Secured Chat iOS App</li> </ul>	
1.4		<p><u>Scalability</u></p> <p>(a) Shall support to minimum of 20,000 users/devices in production environment</p> <p>(b) Shall support concurrent API sessions of upto</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		1,00,000 or higher	
1.5		<u>Network</u> (a) The mobile chat application is expected to work on all the commercial networks 2G/3G/4G and Wi-Fi provided availability of the network  (b) Shall capable of switching to SMS carrier for messaging when internet connectivity is not available for predefined time	
1.6		<u>Availability</u> (a) The mobile app to be available on enterprise store in the form of APK for Android and IPA for iOS  (b) Users can download the mobile apps from the location and install using OTP for pre-registered numbers  (c) The web application for admin console will be available for the internal administrators from all the types of modern HTML5 compliant browsers Internet Explorer, Chrome, FireFox, Safari etc.	
1.7		<u>Server Software Upgrades</u> (a) All upgrades to managed remotely to make the process seamless  (b) The server upgrades will be easily available to the customer  (c) The expected downtime will be minimum for the upgrades	
1.8		<u>Mobile App Upgrades</u> (a) The client (mobile) software to have the intelligence to determine any upgrades on the server and auto update itself with user permission  (b) The chat application to be designed to detect new upgrades and auto update itself.	
1.9		<u>High Availability</u> (a) Shall provide High-Availability deployment (b) Shall support active-active Servers in HA with load-balancing support (c) Shall support site resiliency	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
1.10		<p><u>Hardware Sizing</u></p> <p>(a) Hardware sizing and deployment view along with the option of high availability to be provided in a separate document</p> <p>(b) Shall support ESXi, Hyper-V, KVM based hypervisors</p>	
2	<b>Business Integration</b>	<p><u>Integration with SIMHA Components</u></p> <p>(a) ICG defining a common platform named as SIMHA across organization that will serve their internal apps and portal</p> <p>(b) The proposed solution should be designed to support the SIMHA components or framework</p> <p>(c) Shall provide bi-directional broadcast messages, one-to-one messages from intranet to internet through military grade Data Diodes such as Owl/FoxIt Data Diodes</p>	
2.1		<p><u>Support IAM</u></p> <p>(a) Shall support and integrate with ICG Identity And Access (IAM) Management server</p> <p>(b) Shall support Single Sign On (SSO) implementation through ICG EMM platform</p>	
2.2		<p><u>Support ACL</u></p> <p>ICG also plans to implement Access Control Layer (ACL) across the entire organization and their internal portals and apps. The proposed solution should be designed to support ACL in future when ICG implements.</p>	
2.3		<p><u>Advanced Integration Capabilities</u></p> <p>The system can connect to any internal or external system with API exposed in RESTful forms.</p>	
2.4		<p><u>Integration with Mobile App Management (MAM)</u></p> <p>Design, implementation of Chat application with MAM/MDM with single management console and should be be integrated through RESTful APIs.</p>	
2.5		<p><u>Support RESTful APIs</u></p> <p>(a) APIs should be available for common chat functions such as manage users, manage message, manage user groups through 3rd party software applications</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		<p>(b) Shall support integration of Secure Chat application with various ERP, Middleware, and Bespoke build software applications</p> <p>(c) Shall support integration with Artificial Intelligence based Chat-bots</p>	
3.0	<b>Platform Support</b>	<p><u>Android</u></p> <p>(a) The chat app should work on all the Android devices with version 4.2 onwards</p> <p>(b) Android app has a very intuitive look and feel and all the features and functionality are very easy to use</p> <p>(c) Shall provide responsive GUI design</p> <p>(d) Shall provide authentication using ICG EMM</p>	
3.1		<p><u>iOS</u></p> <p>(a) The chat app should work on all the iOS devices with version 9 onwards</p> <p>(b) iOS app has a very intuitive look and feel and all the features and functionality are very easy to use</p> <p>(c) Shall provide responsive GUI design</p> <p>(d) Shall provide authentication using ICG EMM</p>	
3.2		<p><u>Third-party Containerization Support</u></p> <p>Mobile Chat App must have the ability to further run in secured third party containers</p>	
4.0	<b>Branding</b>	<p><u>Co-branded Apps</u></p> <p>(a) The app component must have ICG specific branding</p> <p>(b) TAPPS (Tatrakshak APPS) is possible for the mobile chat app and the web console</p> <p>(c) Mobile Chat App for both Android and iOS must have TAPPS branding</p> <p>(d) Admin Web Console must have TAPPS branding.</p>	
5.0	<b>Source Code</b>	<p><u>Source Code</u></p> <p>(a) Source Code along with documents to be provided to ICG for non-COTS products</p> <p>(b) Source Code of COTS product should have</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		<p>certified for security by STQC/ CERT-IN empaneled vendors. ICG is entitled to get security audit by any reputed security auditors at any point-in-time as desired. To qualify as COTS product, offered product should have atleast 10 deployments in India each of not below 1,000 Users, should have roadmap for next 05 years, should have atleast 03 channel partners in India with each having atleast 01 current client.</p>	
6.0	<b>Console Functionality</b>	<p><u>Chat Admin Console</u></p> <p>(a) Chat admin console is a web based console that has the Dashboard and view of all the activities and management tools</p> <p>(b) Admin can view latest stats for the chat active users, groups, usage, etc.</p> <p>(c) Admin can add/import users, manage user chat groups, manage policies for chat group and broadcast messages to users.</p> <p>(d) Admin can also configure the Encryption details, Intruder detection and audit approver.</p>	
6.1		<p><u>Integration with ICG HR application</u></p> <p>(a) Support User add/delete/update to be from HR database through RESTful API</p> <p>(b) Support User Group add/delete/update and add/remove Users into User Group based on HR database through RESTful API</p> <p>(c) Provide required management console for User, Group management for integration into ICG HR database</p>	
6.2		<p>Dashboard</p> <p>(a) View Online users</p> <p>(b) Active Users and Conversations</p> <p>(c) User registration status</p> <p>(d) Network Usage statistics</p> <p>(e) Top Active groups</p> <p>(f) Top Active users</p> <p>(g) Total Users, registered chat users, total chat groups</p> <p>(h) Session performance by User/ Device</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		categories. Performance analysis includes query responsive time, sessions per minutes etc.	
6.3		<p><u>Device Analytics</u></p> <p>(a) Device app analytics need to be collected periodically for the various users and displayed on the dashboard as aggregate reports.</p> <p>(b) The reports should include performance metrics like CPU usage, storage, and RAM usage and crash reports.</p> <p>(c) Define the threshold based on the lab testing and latest device available based on CPU and RAM configuration</p> <p>(d) Dashboard – Define duration min to days, Aggregate - criteria (e.g. 1 hr.) , type (crash, active users, performance)</p>	
6.4		<p><u>Manage Organization</u></p> <p>(a) Shall have ability to manage the organizational entities related to users including Department, Designation, Role , Grade, Location, Admin role etc.</p> <p>(b) Manage functions like Add/Edit/Delete/Import/Export for the above entities.</p> <p>(c) Import to be available in CSV format.</p>	
6.5		<p><u>Manage Users</u></p> <p>(a) Enterprise users managed and updated by the Admin, through Admin interface on console</p> <p>(b) Super Admin will define the rights and privileges for other Admins and all users as admin types</p> <p>(c) Manage functions like Add/Edit/Delete/Import/Export users</p> <p>(d) Import to be available in CSV format.</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
6.6		<p><u>Manage Chat Groups</u></p> <p>(a) Admin can view and manage the list of chat groups that are available within the organization.</p> <p>(b) Create a chat group, and invite users to start a chat group conversation.</p> <p>(c) A group can be created by an IT admin or an individual user from the device app.</p> <p>(d) Ability to create permanent and temporary chat groups</p>	
6.7		<p><u>Manage Chat Group Policy</u></p> <p>(a) Admin can manage enterprise chat policies and rules applied on the chat group.</p> <p>(b) While creating group admin would like to set policy restrictions for allowing message forward, allow file sharing, evaporated message setting, max size of attachment, and max chat group users, etc.</p>	
6.8		<p><u>Manage Chat Configuration</u></p> <p>(a) Admin can manage the enterprise configuration</p> <p>(b) One-time configuration is available for setting up the encryption settings, intruder prevention settings and the audit approver</p> <p>(c) Other settings such as GCM (Google Cloud Messaging) if required can be done.</p>	
6.9		<p><u>App Control</u></p> <p>(a) App control to provide the feature to remotely block/unblock the users using the chat app only</p> <p>(b) App data wipe is also possible through the app control</p> <p>(c) User personal data will not be deleted, only the data pertaining to the chat app will be deleted.</p>	
6.10		<p><u>Broadcast Message</u></p> <p>(a) Admin can Create/Manage Broadcast messages. Message sent through the Broadcast option to all the users in the organization</p> <p>(b) Recurring message broadcast</p> <p>(c) Administrator or certain privileged users can create a Broadcast and send messages</p>	



Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		(d) The broadcast can also be used as a bulletin board that will provide admin users to broadcast information, alters, news, etc.	
6.11		<p><u>Message Auditing</u></p> <p>(a) Admin can setup up user privileges for auditing of the chat contents across various groups</p> <p>(b) Approval process with approvers (primary and secondary) must be configurable for roles viewing the auditable traffic</p> <p>(c) Approvers should require pass codes or OTP. View/Share the audited messages in HTML format</p> <p>(d) Any message from a one-to-one chat or a group chat can be audited. Auditing requires to fill criteria for what group or user needs to be audited, date range to be audited, etc.</p>	
6.12		<p><u>Contents</u></p> <p>Help, FAQ, User manual/guide, EULA and support information to be published on the web console.</p>	
7.0	<b>Communication</b>	<p><u>Chat Communication</u></p> <p>(a) The app must offer three levels of communication as following:</p> <ul style="list-style-type: none"> <li>(i) One to One Chat</li> <li>(ii) Group Chat</li> <li>(iii) Broadcast Message</li> </ul> <p>(b) All critical communication to be encrypted during transmission and data at rest and on transmission</p> <p>(c) Conversations can be archived, forwarded, and deleted on device app</p> <p>(d) Chat Groups can be created from console and device app</p>	
7.1		<p><u>Communication Types. Types of messages that are supported are.</u></p> <ul style="list-style-type: none"> <li>(a) Text messages</li> <li>(b) Audio messages</li> <li>(c) Video messages</li> <li>(d) Pictures / Images</li> </ul>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		(e) Location information (f) Documents (PDF format only) (g) Evaporated Messages with fixed validity (h) Private Messages (encrypted) (j) Text messages on SMS carrier	
7.2		<u>Contextual Messages</u> (a) App must have contextual message type. User to have ability to create a message type tagged as Geo-fence and/or time-fence (b) Message with attribute geo-fence will be opened only within the fence restriction provided by the sender and not outside fence (c) This message will be received and opened only when the other user(s) or group user(s) are within the fence limit (d) Similar to Geo-fence, another message type should be time-based or time-fenced.	
8.0	<b>Chat Functionality</b>	<u>User Registration/ Enrolment</u> (a) Users will use the application majorly on their personal devices/ Bring Your Own Device (BYOD) case (b) The registration for the chat app to be simple and seamless. User will follow the instructions provided by his/her admin to enroll the Chat app (c) Details of enrollment will be available in email and/or SMS. After downloading the mobile chat application, new user will be able to register to the chat application server by providing the basic information like user email id and password.	
8.1		<u>User Login</u> (a) Login to be achieved through verification of username and password (b) Login authentication should support Single-Sign-On (SSO), TOTP, OTP, Biometric with integration into ICG EMM (c) User will have to enter the corporate email id and the password to login to the application.	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
8.2		<u>Biometric/Finger print Support</u> Biometric authentication for login, private message and app pin.	
8.3		<u>Forgot Password</u> Forgot password option to be available by which the user will be able to receive the link to change the password with a valid email mechanism.	
8.4		<u>App Lock</u> A numeric PIN must be available to lock the app. This is optional and user can set this PIN from the settings. If the user revisits the app if the app is in background or restarted the user should be prompted for the PIN. The same PIN can be reused for the private message.	
8.5		<u>Chat Home</u> (a) Chat home icons should distinguish between a one-to-one chat and group chat default icons. Chat home will be the home view of recent chats, contacts, groups, search and settings. From home, user will be able to navigate to initiate one-on-one chat or group chat. Following are the functionality from the chat home (i) Search for text within contacts, messages, group's chats, and file caption (ii) Recent Chats displays the recent chat with the most recent at the top conversations with users and within groups (iii) Contacts to display list of Contacts for the user (iv) Status shows the user's current status in the application. The status can be changed from the settings configuration.	
8.6		<u>Moderated</u> Easily moderated by administrator to promote a business only focus	
8.7		<u>User Presence</u> User can view the other users online or offline status.	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
8.8		<p><u>Settings</u>            Settings will have Profile, Wallpaper, Notifications, App Upgrade, Security, and Help, About, FAQ, Contact us. Profile pic can be updated by adding a new pic or click a new photo. User can update his/her status message. User can also change password from the settings section. App lock and Private message PIN can be set from here. Settings will also enable user to set/change password and logout from App.</p>	
8.9		<p><u>Individual Device Preferences</u>            Set separate preferences for mobile environments e.g. profile, alert notification, tone.</p>	
8.10		<p><u>Evaporated/ Self-destructive Message</u>            Evaporate messages are type of messages which will be self-destructive or auto-deleted after a set period of time. Time could be configured as minutes, hours. User can set the expiry time while sending an Evaporated text/audio and/or video message to individuals or on a Group chat. These messages will be tagged as evaporated messages on the server and while delivering to the other users displayed in a special iconic form that distinguishes it from a normal message. Post expiry messages should automatically get deleted/hidden from the device.</p>	
8.11		<p><u>Private Message</u>            Private messages are type of message which can be viewed ONLY with a numeric PIN. User can send a message as a private message option. PIN needs to be set to view the private message. The PIN can be set from the setting section. If PIN not set, the system will force user to set the PIN. On entering correct PIN all the private messages will be displayed until the user is on that chat conversation window. Private messages are applicable for 1-1 and group chat. Special icon will be displayed for private message. By default, private messages are encrypted. User can also combine evaporated message as private message.</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
8.12		<p><u>One-to-one Chat</u></p> <p>User will be able to do one to one chat with any other user available in the list of contacts. Within the chat, share images, audio, video and files from selected folder will be possible. Messages sent will have the message info time stamp, indicators for status of the message like pending, sent, delivered, read. Chat Info will display the contact Info following name of the contact (icon if added), online status message, media shared if any, email, phone no, etc.</p> <p>User will be able to share location to any other user. The location will be received in the form of latitude and longitude coordinates. The receiver of this location will be able to view the location in a map.</p>	
8.13		<p><u>Group Chat</u></p> <p>User will be able to do group chat with multiple user available in the group. Within the chat groups, user will be able to share images, audio, video and files from selected folder. Group Chat messages are distinguished based on group icon or profile pic of the group. Messages sent within the group will have the message info time stamp, indicators for status of the message like pending, sent, delivered, read, and/or failed. Group Chat Info will display the contact Info following name of the group (icon if added), create date, members within the group, media shared if any, etc. Limited group size is allowed ~ 250 users.</p>	
8.14		<p><u>Message Delivery Status</u></p> <p>(a) User need to have a status of the messages that are delivered within a chat or group chat. User will be able to view the status of messages are delivered, read by the other users. This is applicable for messages sent within chat and group chat both. Status to be displayed with date/time</p> <ul style="list-style-type: none"> <li>(i) Pending</li> <li>(ii) Sent</li> <li>(iii) Delivered</li> <li>(iv) Read</li> </ul> <p>(b) Indicators on messages should display if the</p>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
		messages are delivered, read etc. This functionality should be real time.	
8.15		<p><u>Chat History</u></p> <p>User be able to view and delete/clear chat history. This is applicable for both the chat and the group chat feature. Users can view an archived collection of the chats from the settings menu. All the active chat tab lists open chat conversations, including one on one and group chat, ordered by the received time of the latest message.</p>	
8.16		<p><u>Secure Vault</u></p> <p>(a) Secured Vault is a secured application workspace for storing images, audio, video, files. Vault will be protected for the contents that lie within the chat app vault and no other app on the device will be able to access the contents. The contents from the vault will not be available to view using any file explorer or browser. Vault in the Chat app will secure the data and data cannot be leaked in any circumstances from this vault.</p> <p>(b) Messages and contents not to be shared outside the app, but any data from outside can be copied into the chat app.</p> <p>(c) Basic PDF, images, video and audio file type to be supported.</p>	
8.19		<p><u>In-App Viewer</u></p> <p>(a) Following are the in-app viewers must be available for displaying the different type of contents of the app.</p> <ul style="list-style-type: none"> <li>(i) Image Viewer</li> <li>(ii) Audio Player</li> <li>(iii) Video Player</li> <li>(iv) PDF File Viewer</li> <li>(v) URL (web-viewer)</li> <li>(vi) Location (map-viewer)</li> </ul>	

Sl.	Category	Technical Requirements - Secure Chat	Complied (Yes/ No)
8.20		<p><u>Sync Contacts</u></p> <p>Show all the contacts from the company including their full name, email id and contact no. Search available to search contacts based on name, email and mobile number. The initial list of contacts to be pre-loaded or synced with the phone book contact list.</p>	
8.21		<p><u>Search</u></p> <p>User must be able to search for any text in chat conversations, contacts, names, messages, and file captions.</p>	
8.22		<p><u>Message Archiving</u></p> <p>Archiving and un-archiving of chat conversations</p>	
8.23		<p><u>Message Archiving</u></p> <p>(a) Secure Chat users shall be able to invoke encryption facility to encrypt an outgoing message. Only the intended recipient of a message will be able to open and read the message. We use hybrid encryption i.e. combination of symmetric and asymmetric encryption algorithm.</p> <p>(b) Encryption degrades the user experience; hence it is recommended that encryption should be used sparingly and only when really required</p> <p>(c) Files attached to messages will be encrypted</p> <p>(d) These are known as private message with file attachments. Basic scope is to support only PDF files along with media files.</p>	
8.24		<p><u>Notifications Settings</u></p> <p>Set alerts for chat and group messages. User must be able to set notifications to alert you with sound, vibration when someone begins a chat.</p>	
9.0	<b>Support</b>	<p><u>Support Team</u></p> <p>Support team to be ready available for any questions and aid in troubleshooting. Contact numbers to be provided to avail any support.</p>	
9.1		<p><u>User Guides</u></p> <p>Full catalogue of user guides available in different formats must be available.</p>	





Section-B –**Unified Endpoint Management Software**

<b>Sl.</b>	<b>Category</b>	<b>Specification</b>	<b>Complied (Yes / No)</b>
1.0	<b>Key Capabilities</b>	Should offer mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM) capabilities	
1.1		Should provide data-in-rest, data-in-process and data-in-transfer security for ICG applications, data on mobile devices including Android, iOS, Windows OS devices	
1.2		Should support ICG applications lifecycle on mobile devices including publishing, updating, removing within secured application container	
1.3		Configure, manage and monitor iOS, Android, Windows 10 and macOS, and manage some Internet of Things (IoT) and wearable endpoints	
1.4		Unify the application of configurations, management profiles, device compliance and data protection	
1.5		Provide a single view of multidevice users, enhancing efficacy of end-user support and gathering detailed workplace analytics	
1.6		Act as a coordination point to orchestrate the activities of related endpoint technologies such as identity services and security infrastructure	
2.0	<b>Device support</b>	The Solution should support mainstream mobile and tablet Operating Systems (OS), like iOS and Android.	
3.0	<b>Management</b>	The Solution should provide web- based admin console to render visibility into all devices and applications. Product should have the provision for necessary customization.	
3.1		The solution should provide role-based access and views for management console	
3.2		The solution should allow users to help themselves with a self-service portal with one-	

Sl.	Category	Specification	Complied (Yes / No)
		time passcodes and server auto-discovery	
3.3		The solution should provide quick view into real-time deployment data from the admin console	
3.4		The solution should provide a comprehensive list of devices and drill down into specific device and user details.	
3.5		The solution should Send commands (such as include device query, clear passcode, send message, lock device, set roaming, remote view, sync device) on demand to devices to request information and perform action Commands	
3.6		The solution should allow to create reports including unmanaged devices, compliance reporting, app and device inventory and system alerts	
4.0	<b>Authentication</b>	The Solution should provide real-time integration with directory services (AD/LDAP) to fetch existing directory services structure into the solution such that changes in the AD/LDAP are synchronized with the solution	
4.1		The Solution should authenticate against Active directory/LDAP, one time passcodes or Security Assertion Markup Language (SAML) based Authentication	
4.2		The Solution should provide multi factor authentication integrated with third party MFA (Biometric/ OTP based solutions).	
4.3		The solution should enhance user experience by enabling PIN based authentication for secure applications	
4.4		The solution should provide support for Touch ID offline authentication.	
4.5		The solution should have the ability to define a passcode for the corporate applications	
5.0	<b>App Delivery</b>	The solution should be able to provide containerized corporate applications without	

<b>Sl.</b>	<b>Category</b>	<b>Specification</b>	<b>Complied (Yes / No)</b>
	<b>Management</b>	device enrolment or MDM solution	
5.1		The solution should provide an internal app distribution mechanism (customized app store) and provides a way to create and manage app catalogue securely.	
5.2		The solution should cloud based or integrated app wrapping solution	
5.3		The solution should support distribution of secure apps thru public stores	
5.4		The solution should have the ability to restrict deployment of corporate applications on rooted or Jail broken devices	
5.5		The solution must provide versioning and seamless rollback to prior app versions from the administrator console	
6.0	<b>Data Management</b>	The solution should provide an integrated tool to create and edit documents, presentations, spreadsheets, and image files and annotate PDF	
7.0	<b>Integration</b>	The solution should tested and certified with secure chat application	
7.1		The solution should provide seamless plug in to existing IT infrastructure including LDAP, PKI, NAC, VPN, Wi-Fi and SIEM	
7.2		The solution should provide dynamic containerization of applications from public store	
7.3		The solution should provide capability to integrate with third party tools to use REST API.	
8.0	<b>SDK and Toolkit</b>	The solution should provide application wrapping and application containerisation with same set of features	
8.1		The solution should enable containerisation of any app with SDK	
8.2		The SDK should add security features with	

Sl.	Category	Specification	Complied (Yes / No)
		Single line of code	
9.0	<b>Security</b>	Should provide app level encryption through app micro-VPN and should not rely on device level encryption	
9.1		Should support device level VPN	
9.2		The solution should separate personal and private user data from business data	
9.3		All contents generated/ used by ICG apps within app container must be encrypted by AES 256 or equivalent while data-in-rest, and data-in-transfer	
9.4		The solution should provide integrated application wrapping capability to provide business app containerization (sandboxing), secure app data encryption and apply security polices to the app to prevent data leakage.	
9.5		The solution should have the ability to restrict corporate application deployment on the device if device passcode is not enabled	
9.6		The solution should have controls to prohibit opening of app when network connectivity is not available.	
9.7		The solution should be able to define the maximum number of hours that a corporate app can be access in on offline mode. After this timeout the application will mandatorily need to come online and sync with the corporate policies	
9.8		The solution should provide the user a grace period for updating their corporate apps. The users may choose to upgrade over their cellular network or Wi-Fi network. After the expiry of grace period the application should be forcefully updated	
9.9		The solution should have the ability to erase application data in scenarios where the device is locked by the administrator or a user using self-service portal.	

Sl.	Category	Specification	Complied (Yes / No)
9.10		The encryption of the corporate application should be based on user input parameters like user credential and device parameters. The encryption should not be through MDM based device encryption	
9.11		The solution should provide a Secure, encrypted access to intranet sites via app specific VPN. Solution should provide Secure Network Access to corporate resources without any additional client	
9.12		The solution should provide a Linux based secure gateway for authentication and app specific VPN tunnel.	
9.13		The solution should encrypt data-at-rest and data-in-motion	
9.14		The solution should have the ability to define inter-app communication on an individual application basis	
9.15		Shall restrict copy and cut. Here the data copied in the corporate app should be placed in a separate corporate clip board for use with other corporate apps	
9.16		Shall restrict clipboard paste operation. Here the solution should be able to define if the paste operation is from the corporate clipboard or generic device clipboard	
9.17		Shall restrict document/attachment opening in apps not controlled by the mobility platform	
9.18		Shall provide exception for certain document types to use apps not controlled by solution.	
9.19		Shall block connections to the corporate apps based on compromised ciphers like SSL v3	
9.20		Shall block camera access for certain corporate apps based on defined active directory user groups	
9.21		Shall block Photo Library access for certain corporate apps based on defined active	

Sl.	Category	Specification	Complied (Yes / No)
		directory user groups	
9.22		Shall block microphone access for certain corporate apps based on defined active directory user groups	
9.23		Shall block dictation services for certain corporate apps based on defined active directory user groups	
9.24		Shall block GPS services for certain corporate apps based on defined active directory user groups	
9.25		Shall block file backup services for certain corporate apps based on defined active directory user groups	
9.26		Shall block printing capabilities for certain corporate apps based on defined active directory user groups	
9.27		Shall block file attachments for certain corporate apps based on defined active directory user groups	
9.28		Shall obscure screen contents for all corporate apps when the user switches between multiple apps on his device+E84	
9.29		Shall block IOS specific services like iCloud and airdrop for all corporate apps based on defined active directory user groups	
9.30		Shall define the network access mode for each corporate app by choosing between tunnelled network connection to customer DC, open internet access and complete network isolation	
9.31		Shall have application level geo-fencing capabilities where by certain corporate applications will only be permitted to be accessed in certain locations for e.g. certain apps can only be used in the customer campus	
10.0	<b>Corporate browser capabilities</b>	The corporate browser should be compatible with IIS, WebSphere and LAMP stacks	

Sl.	Category	Specification	Complied (Yes / No)
10.1		the corporate browser should have the ability to whitelist and black list URL's	
10.2		The solution should have the ability centrally push bookmarks to the corporate browser	
10.3		The solution should have the ability to define the home page for the corporate browser	
10.4		The solution should have the ability to block password caching on the corporate browser	
10.5		The solution should allow to save pages offline and access offline pages using 3D touch	
10.6		The solution should be able to encrypt browser cache, bookmarks, cookies and history	
10.7		Shall provide mobile client Enterprise Anti-Virus protection for Android & iOS through 3 <sup>rd</sup> party solution integration	
11.0	<b>Email Client capabilities (for ActiveSync)</b>	The Email client should be compatible with IOS operating system	
11.1		The Email client should be compatible with Android operating system	
11.2		The Email client should be compatible with Exchange Active Sync	
11.3		The Email client should provide Integrated email, calendar and contacts with simple, intuitive and native user experience	
11.4		The mail server URL should be pre-populated in the mobile email client	
11.5		The Email client should support the ability to support contact sync with exchange	
11.6		The email client should support the ability to support calendar sync with the ability to view team calendars	
11.7		The Email client should have the ability to set out of office	

<b>Sl.</b>	<b>Category</b>	<b>Specification</b>	<b>Complied (Yes / No)</b>
11.8		The email client should support user created folders in the mailbox	
11.9		The users should be able to select duration for which emails are available in the mobile email client	
11.10		Automatic notifications of new email or calendar events	
11.11		Solution should have ability to open attachments from calendar events	
11.12		Ability to view free/busy status in calendar and forward meeting invitations	
11.13		Multi-select emails for bulk operations	
11.14		Solution should support sending of files to Secure Email Client from MDX apps	
11.15		Solution should support to attach emails as attachments (.msg and .eml files)	
11.16		Solution should provide email attachment encryption to ensure complete Data Leakage Protection	
11.17		The email client should allow to add multiple email accounts	
11.18		The email client should provide swiping gestures like mark, flag email and/or delete	
11.19		The client should provide information about conflicting events on personal calendar	
11.20		The email client should be able to send, receive, open and save .zip file attachment	
11.21		The email client should support intelligent Scheduling assistant with suggestions	
11.22		The calendar should allow attachments included in meeting events to be saved for offline access	
12.0	<b>Security Certifications</b>	The Solution should have comprehensive predefined security configuration assessment	



<b>Sl.</b>	<b>Category</b>	<b>Specification</b>	<b>Complied (Yes / No)</b>
		checks (settings) for different supported platforms as per industry standards including FIPS 140-2.	
13.0	<b>Brand reputation</b>	Should have been leader quadrant in latest Gartner Magic Quadrant, Forrester IDC Reports	
14.0	<b>Deployment and Licensing</b>	The solution should support both cloud based and on-premise deployment	
14.1		The solution should support perpetual licenses	
15.0	<b>Support</b>	The OEM should provide 24x7 online support	

Section-C **Composable IT Infrastructure with SDDC**

<b>Srl.</b>	<b>Parameters</b>	<b>Technical Requirements for Composable IT Infrastructure</b>	<b>Complied (Yes/No)</b>
<b>1.0.0</b>	<b>General Requirements</b>	<b>Composable IT Infrastructure</b>	
1.1.0	Fluid resource pool	Disaggregated resource control to enable abilitys to independently scale resources including memory, storage and compute	
1.1.1		Compute, storage and networking resources should be fluid, separated from underlying physical infrastructure and independent of each other	
1.1.2		Proposed solution should support heterogeneous platforms that includeESXi, Hyper-V , Oracle VM Server, Linux KVM, Openstack hypervisors and next generation containers and Bare metal servers concurrently on the same cluster	
1.1.3		Solution should provide the flexibility to either combine the compute and storage functions on the same hardware or separate the compute and storage functions into different tiers. Irrespective of the mode of deployment, the cluster should be managed using a single GUI	
1.1.4		Should provide unified single GUI to manage fluid resource pool	
1.2.0	Scalability	Proposed solution should be scalable upto 1000 nodes in a single cluster	
1.2.1		Linear scalability of IT resources	
1.3.0	API driven IT	Support 'Infrastructure-as-Code' that allows computing resources to be provisioned with code, eliminating the need to physically configure hardware to meet the needs of new or updated applications	
1.3.1		Enables developers to programmatically deploy new virtual machines and other structures so that they can more quickly test their code	

Srl.	Parameters	Technical Requirements for Composable IT Infrastructure	Complied (Yes/No)
1.3.2		Allows an application to automatically instantiate new infrastructure based on performance conditions at the present time	
1.3.3		Enables automation-based user self-service, and provide 'Private Cloud' services	
1.3.4		Support DevOps	
1.4.0	OEM Certification	Should be certified for deployment by OEM of MAM being offered to ICG	
1.5.0	SDDC Support	Should support Software Defined Data Center (SDDC), detailed requirements are as defined in succeeding specifications	
1.5.1		The solution should provide software based enterprise class storage services on server hardware available from all the leading server vendors in the industry. It should support both hybrid and all flash configurations on the server	
1.6.0	Support	Hardware and Software support to be from the same, single OEM and not outsourced from any third party, either licensed or non-licensed	
1.7.0	Performance	Proposed solution should be capable of providing 2,00,000 IOPS per node in the environment	
1.7.1		Solution should be able to provide under 2 millisecond latency	
1.7.2		80TB Backup should be completed in 8 hour window	
1.7.3		The proposed solution should support NVMe SSD disks	
1.7.4		The proposed solution should support 500GB or more of memory per node	
1.7.5		The proposed solution should support SIX 9's of High Availability	

Srl.	Parameters	Technical Requirements for Composable IT Infrastructure	Complied (Yes/No)
1.8.0	Others	Proposed solution should ensure best performance by leveraging all the drives in the cluster for I/O and not depend on the locality of data	
1.8.1		Proposed solution should have the ability to scale compute and storage together or individually in the same cluster	
1.8.2		Proposed solution should optimize the storage capacity consumption without creating independent workload islands within a single cluster	
1.8.3		A redundant copy of the data is to be maintained at all times within a cluster and distributed in such a way that the cluster can withstand a disk drive or a node failure	
1.8.4		In the event of a node/disk failure, the system should initiate redundant copy creation of data in the free space without requiring a spare node/disk	
1.8.5		Should support the Dial home feature to proactively alert of failures	
1.8.6		The solution should support the seamless upgrade of storage controller capabilities and storage	
1.8.7		The solution should allow common management across storage tiers. It should support the migration of volumes between storage tiers	
1.8.8		Software defined storage fault domains provide the ability to tolerate rack failures in addition to disk, network and host failures.	
1.8.9		Solution should support an all-flash architecture delivering consistent, predictable performance with sub-millisecond response times with appropriate disks/SSDs.	
1.8.9		Provider REST API interface to enable the automation of operations through an external management tool	
1.9.0	Compute Node	(b) Intel Xeon Gen10 or latest (c) Processor cache 38 MB or higher (d) DDR4-2666 NVDIMM or higher	

Srl.	Parameters	Technical Requirements for Composable IT Infrastructure	Complied (Yes/No)
		(d) NVMe SSD, 12 G (e) Memory should feature Advanced ECC, Memory Mirroring Mode and Memory Online Spare (f) Silicon Root-of-Trust inbuilt into System-on-Chip	
1.10.0	Storage Node	(a) Support minimum of 30 SFF of 12G SAS/6G SSD (b) Capacity to be scalable upto 100 TB or higher per node (c) Storage be provided in NL-SAS HDD	
<b>2.0.0</b>	<b>SDDC-Native Cloud</b>	<b>Composable IT Infrastructure</b>	
2.1.0	Automation & Provisioning	The solution should be able to automate and provision data-center services such as compute, storage, networking, backup, replication, load balancing, fault tolerance, security, firewall, etc.	
2.2.0	Self-Service Portal	The solution shall provide a web-based self-service portal for IT/Business users to request for services. Solution should provide unified service catalogue where users can request and manage personalized IT services so that each user gets the right size service with right SLA based on their business requirement with support for multi hypervisor environment including vSphere, Hyper-V, RHEV and XEN	
2.3.0	In-built HA	Cloud solution components should have inbuilt High-Availability(HA) functionality without any dependency for all integral elements	
2.4.0	Governance	The solution shall support Governance via multiple levels of approval integrated with email notifications such that approvals/rejections can be done without having to login to the self-service portal	
2.5.0	Visual workflow design/Orchestration	The solution should provide visual drag-and-drop interface for developing custom workflows at the Orchestration layer. The visual workflow designer should enable activities to be easily inserted into a workflow.	

Srl.	Parameters	Technical Requirements for Composable IT Infrastructure	Complied (Yes/No)
2.6.0	Unified management	The solution shall provide a unified management of performance, capacity and compliance for the proposed platform with the ability to identify and report on over-sized, under-sized, idle and powered-off virtual workloads	
2.7.0	Service Discovery & Service Mapping	The solution should have the ability for Service Discovery and Service mapping in virtual environment, examine the application discovery status, view and analyze the dependency. It provides a centralized view of the application environment	
2.8.0	Log analysis	The solution should be able capture events and logs from 3rd party sources like servers, storage, OS, Applications near real time to perform log analysis and provide out of box dashboards for time series based log analysis	
2.9.0	OpenStack Integration	Shall natively integrate with 'Enterprise OpenStack' and support multiple hypervisors of VMware ESXi, Microsoft Hyper-V , Oracle VM, Xenserver and KVM	
<b>3.0.0</b>	<b>SDDC-Virtualisation</b>	<b>Composable IT Infrastructure</b>	
3.1.0	Bare metal Hypervisor	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	
3.2.0	Live storage migration	Virtualization software should have the ability to live migrate Virtual machines files from one storage array to another without any Virtual Machine downtime. It should support this migration from one storage protocol to another (ex. FC, iSCSI, NFS, DAS)	
3.3.0	Continuous Availability	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.	

Srl.	Parameters	Technical Requirements for Composable IT Infrastructure	Complied (Yes/No)
3.4.0	High-Availability	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 automatically restarted to another physical server running same virtualization software. The feature should be independent of Guest Operating System Clustering and should work with FC/ iSCSI SAN and NAS shared storage.	
3.5.0	Native Storage API integration	The solution should provide special integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.	
3.6.0	Virtual native NGFW integration	The solution should provide option for securing virtual machines with offloaded antivirus and antimalware solutions without the need for agents inside the virtual machine with integration with 3rd party Anti-Virus/Anti-Malware solutions	
3.7.0	End-to-end cloud delivery	Proposed Virtualisation and cloud automation solution should be from the same OEM offering key components ( like Self-service catalogue, Cloud portal, Orchestration, intelligent operations management & monitoring, log analytics, chargeback/show back etc.) with out of box integration capabilities.	
<b>4.0.0 SDDC - Network Virtualisation Composable IT Infrastructure</b>			
4.1.0	Distributed in-kernel routing	The solution should provide distributed in-kernel routing. So the Routing between Virtual Machines with different IP subnets can be done in the logical space without traffic going out to the physical router.	
4.2.0	Provisioning of network services	Provisioning of virtual/ software defined network services should be possible irrespective of make and topology underlying physical network switches and routers.	
4.3.0	Live migration of security	The Security policies must follow the VM in the event of migration (i.e. live migration)	

<b>Srl.</b>	<b>Parameters</b>	<b>Technical Requirements for Composable IT Infrastructure</b>	<b>Complied (Yes/No)</b>
	policies		
4.4.0	SD Security	The solution should be capable to provide agent based or agentless guest introspection services like Anti-Malware etc. and Network introspection services like IPS/IDS etc.	
4.5.0	Native integration with 3 <sup>rd</sup> party security solutions	The solution should offer to Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services.	
4.6.0	Network Function Virtualisation (NFV)	The solution should offer to deploy virtualized network functions (like switching, routing, firewalling, VPN, DHCP and load-balancing), Web Application Firewall (WAF). Administrators can build virtual networks for Virtual Desktop Infrastructure without the need for complex VLANs, ACLs, or hardware configuration syntax on physical network.	
4.7.0	Link encryption	The solution should provide Industry-standard IPsec and SSL VPN capabilities that enables securely extending the virtual datacenter. This Site-to-site VPN support would link virtual datacenters and enable hybrid cloud computing at low cost. The SSL VPN capability would deliver remote administration into the virtual datacenter through a bastion host, the method that is favored by auditors and compliance regulators.	
4.8.0	Clustering across data center	The solution should enable technology for network virtualization, providing network abstraction, elasticity and scale across the datacenter. It should provide technology to scale applications across clusters and pods without any physical network reconfiguration	
<b>5.0.0</b>	<b>SDDC - Compute Virtualisation</b>	<b>Composable IT infrastructure</b>	



<b>Srl.</b>	<b>Parameters</b>	<b>Technical Requirements for Composable IT Infrastructure</b>	<b>Complied (Yes/No)</b>
5.1.1	Data Protection	Compute node should have dedicated cache in raid controller for data protection	
5.1.2	Power Supply	High-efficiency, hot-plug, Platinum Efficient redundant power supplies	
5.1.4	OS Support	(a) Microsoft Windows Server 2016 Standard/Data Center Edition (b) Novell SUSE Linux Enterprise Server (c) Red Hat Enterprise Linux	
5.1.5	Availability	ECC memory, hot-plug hard drives, hot-plug redundant cooling, hot-plug redundant power, tool less chassis, support for high availability clustering and virtualization, proactive systems management alerts	
5.1.6	Management	(a) Should be provided along with server from server OEM only (b) Agent Free monitoring (c) Should support redundant fail safe hypervisor for Virtualization platform (d) IPMI 2.0 compliant	

Section-D - **Tape Library**

<b>Srl.</b>	<b>Technical Specifications – Tape Library</b>	<b>Compliance (Yes/No)</b>
1.0	Offered Tape Library shall support Native data capacity of minimum of 280TB (uncompressed) expandable to minimum of 700TB (2.5:1compressed) using LTO-7 Technology.	
2.0	Tape Library shall provide web based remote monitoring capability.	
3.0	The Tape Library unit shall be configured with 4 FC LTO Gen-7 Tape Drives.	
4.0	Tape Library shall be scalable to four FC LTO-7 drives within the same frame.	
5.0	Offered tape library shall be offered with minimum of 12 Cartridge slots and barcode reader	
6.0	Tape Drive Architecture in the Library shall conform to INCITS/T10 SCSI-3 standard or newer standards.	
7.0	Offered LTO-7 drive in the Library shall conform to the Data rate matching technique for higher reliability.	
8.0	Offered LTO-7 drive in the library shall offer optional WORM support and embedded AES 256 bit encryption.	
9.0	Offered Library shall be provided with a hardware device like USB key, separate appliance etc. to keep all the encrypted keys in a redundant fashion.	
10.0	Offered LTO-7 drive shall have native speed of 300MB/sec.	
11.0	Offered tape Library shall have partitioning support and shall support at-least two number of partition so that configured drives can have owned partition and slots.	
12.0	Tape Library shall provide native Fiber connectivity to SAN Environment.	
13.0	For optimal Performance. Tape Library shall provide native 8Gbps FC interface connectivity to SAN switches.	
14.0	Tape Library shall be offered with minimum of 12 slots and barcode reader.	

<b>Srl.</b>	<b>Technical Specifications – Tape Library</b>	<b>Compliance (Yes/No)</b>
15.0	Tape library shall support removable magazine and mail slot.	
16.0	Tape Library shall have GUI Front panel.	
17.0	Tape Library shall have option for redundant power supply.	
18.0	Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.	
19.0	Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.	

Section-E – **Rack Server**

Sl.	Category	Technical Requirements for Rack Server	Complied (Yes/ No)
1.0	<b>Compute</b>	(a) Intel Xeon Gen10 or latest (b) Processor cache 25 MB or higher (c) DDR4-2666 NVDIMM or higher (d) Memory should feature Advanced ECC, Memory Mirroring Mode and Memory Online Spare	
2.0	<b>Storage</b>	(a) Support minimum of 04 SFF 12G SAS/ 6G SSD (b) Capacity to be scalable upto 100 TB or higher per node (c) Storage be provided in SAS HDD	
3.0	<b>Network</b>	(a) Provide FC-HBA in High Availability with SAN Switch, Tape Library and Composable IT Infra Chassis (b) Provide FC-HBA in High Availability with Backup Appliance (c) Provide Ethernet ports in HA as required	
4.0	<b>Other Software</b>	(a) Windows 2016 or latest with SA (b) Backup software, 10 VM or 02 Socket (c) Endpoint Protection Software - 01 No. (d) Virtualisation software – 02 Socket	

Section-F **SAN Switch**

<b>Srl.</b>	<b>Technical Specifications – SAN Switch</b>	<b>Compliance (Yes/ No)</b>
1.0	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 12 Ports scalable to 24 ports.	
2.0	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.	
3.0	Should deliver 16 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports in an energy-efficient, optimized 1U form factor.	
4.0	Should protect existing device investments with auto-sensing 4, 8, and 16 Gbit/sec capabilities.	
5.0	The switch shall support different port types such as FL_Port, F_Port, E_Port, EX_Port.	
6.0	The switch should be rack mountable.	
7.0	Offered Switch shall be provided with redundant FAN and shall have option for redundant power supply.	
8.0	Non-disruptive Microcode/ firmware / Software Upgrades and hot code activation.	
9.0	The switch shall provide Aggregate bandwidth of minimum of 768 Gbit/sec end to end in full duplex mode.	
10.0	Switch shall have support for Adaptive Networking services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high-priority traffic.	
11.0	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.	
12.0	SAN switch shall support Fibre Channel Integrated Routing for selective device sharing while maintaining remote fabric isolation for higher levels of scalability and fault isolation.	
13.0	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.	
14.0	The switch shall be able to support ISL trunk up to 128 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.	
15.0	SAN switch shall support to isolate the high bandwidth data flows traffic to specific ISLs.	
16.0	Switch shall support to measure the top bandwidth-consuming	

<b>Srl.</b>	<b>Technical Specifications – SAN Switch</b>	<b>Compliance (Yes/ No)</b>
	traffic in real time for a specific physical or virtual device, or end to end across the fabric.	
17.0	Switch shall have support for web based management and should also support CLI.	
18.0	The switch shall support advanced zoning and ACL to simplify administration and significantly increase control over data access.	
19.0	SAN switch shall have support to configure the switches with alerts based on threshold values for temperature, fan status, Power supply status, port status.	
20.0	Switch shall support POST and online/offline diagnostics, including RASrtrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).	
21.0	The switch should have USB port for firmware download, support save, and configuration upload/download.	
22.0	Offered SAN switches shall be highly efficient in power consumption. Bidder shall ensure that each offered SAN switch shall consume less than 100 Watt of power.	

Section-G – **Virtual Next Generation Firewall with WAF**

Sl.	Category	SD-Security Technical Requirements	
1.0	<b>General</b>	The device should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit corporate credentials based on the site's URL category thus blocking users from submitting credentials to untrusted sites while allowing users to continue to submit credentials to corporate and sanctioned sites.	
2.0	<b>Virtual appliance</b>	The proposed Next Generation Firewall should be in Software Form factor and can be either present in the Virtualization/ Hypervisor layer or as a Virtual Machine	
3.0	<b>Single Policy Rule</b>	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.	
4.0	<b>Single-Pass Architecture</b>	It should have the Single-Pass Architecture approach. The architecture should enable full, contextual classification of traffic, followed by a rich set of enforcement and threat prevention options. The architecture should also classify and control traffic in a "single pass" through the firewall.	
5.0	<b>Native SIEM Integration</b>	The Firewall should be able to integrate on standard protocols with leading SIEM solutions and should natively support minimum of like ArcSight and, Splunk.	
6.0	<b>Security features</b>	The solution must support Routing, load sharing, Firewall, Web Application Firewall (WAF), Application visibility and control,	

Sl.	Category	SD-Security Technical Requirements	
		User ID, IPS, Anti-virus from day one.	
7.0	<b>Application Aware</b>	The solution must provide application identification natively, without requiring any license/subscription/blade, provide real time traffic logs based on applications irrespective of ports. While monitoring real time traffic logs, solution must provide detailed view of Defense Services 's application and Users, not just ports and IP addresses. E.g. the solution must distinguish between telnet on port 80 and http traffic between same pair of source and destinations. The proposed solution must also have capabilities for decrypting SSL and SSH traffic for both inbound (connection across any port and not just 443 and 22) and outbound	
8.0	<b>Multi-Hypervisor Support</b>	The firewall should support following hypervisor and orchestration environments  VMware NSX, KVM with optional support for the OpenStack plugin, ESXi, Hyper-V, Citrix NetScaler SDX	
9.0	<b>Zero-day threat detection using Sandbox</b>	The proposed solution shall provide sandbox behavior based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) in future and the solution shall be able to provide automated signature generation for discovered zero-day malware and the solution should ensure the delivery of the signature in 5 mins from the time of detection. No file has to be shared and the analysis should be done on premise at the central location if required.	
10.0	<b>Performance Requirement at DC &amp; DR</b>	The proposed solution should support from 4 Mbps scalable to 100 Mbps of performance with Firewall, application control, IPS, Anti-Virus and Anti-malware enabled from day-1.	



Sl.	Category	SD-Security Technical Requirements	
10.1		The proposed solution must support 60,000 concurrent sessions and 2,500 new sessions per second. The session count must be active TCP connections. The concurrent sessions must not drop while enabling all requested features and should be scalable to 4 times.	
10.2		The proposed solution must support at least 100 Mbps of IPSEC VPN throughput and 500 IPsec VPN tunnels and 500 SSL VPN Users from Day one without requiring any license.	
10.3		The proposed solution must be in the Gartner Magic Quadrant of Enterprise Firewalls for the last 3 years- 2017, 2016 & 2015.	
11.0	<b>Central Management Software Requirement for Central location</b>	Should be deployed in virtual form factor and group devices into logical, hierarchical for management flexibility and deploy policies centrally to be used in conjunction with regional or functional policies. Delegate appropriate levels of administrative control at the regional level or centrally with role-based management.	
11.1		It should be capable of automatically correlate indicators of threats for improved visibility and confirmation of compromised hosts across network and centrally analyze, investigate and report network traffic, security incidents and administrative modifications.	
11.2		It should be possible to view a customizable graphical summary of security threats, applications, users and content.	
11.3		Should support XML based REST API and should have canned as well as option for customized reports for custom number of days, geographical based reports, top threats, applications etc.	

<b>Sl.</b>	<b>Category</b>	<b>SD-Security Technical Requirements</b>	
12.0	<b>Enterprise Integration and API Security</b>	Should provide RESTful API based integration with Enterprise systems	
13.0	<b>Web Application Firewall</b>	Should protect RESTful API Services, Web Applications from threats such as unauthorised User & Device access	

Section-H – **Private Cloud Virtualisation Software**

Srl.	Parameters	Technical Specification-SDDC for Composable IT Infrastructure	Complied (Yes/No)
1.0.0	<b>Key SDDC requirements</b>	Should provide Software Defined Compute, Storage and Networking	
		Should provide <b>automation &amp; orchestration</b> and support self-service for provisioning/ deprovisioning of Compute/storage/networking on-the-fly	
1.1.0		Enterprise wide centralised ' <b>Single-pane-of-monitoring and management</b> ' from single integrated window	
1.2.0		<b>High-Availability(HA)</b> configuration with no 'Single-point-of-failure'	
2.0.0	<b>Software Defined Compute</b>		
2.1.0	Hypervisor	Virtualization software should be bare metal hypervisor with functionality of High Availability, Fault Tolerance, hot Add (CPU, Memory, Storage & Network), dynamic resource scheduler, distributed switch, dynamic power management, storage and network IO control, VM level encryption	
2.1.1		Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS	
2.2.0	Multi-OS support	Virtualization software shall allow heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu, CentOS and Solaris x86)	
2.3.0	VM migration	Virtualization software should support live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option.	
2.4.0	Hot swap	Virtualization software should provide capabilities of Hot Add (CPU, Memory & devices) to virtual machines when needed, without disruption or downtime in working for both windows and Linux based VMs	

Srl.	Parameters	Technical Specification-SDDC for Composable IT Infrastructure	Complied (Yes/No)
2.5.0	OpenStack API integration	Virtualization solution should have the capability to provide out of box integration with Openstack API's and should support all services of Core Open Stack	
2.6.0	Agentless Endpoint protection	Virtualization software should provide integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, anti-malware solutions without the need for agents inside the virtual machines.	
<b>3.0.0</b>	<b>Software Defined Storage</b>		
3.1.0	Hardware vendor agnostic	The solution should provide software based enterprise class storage services on server hardware available from all the leading server vendors in the industry. It should support both hybrid and all flash configurations on the server	
3.1.1		The solution should have a flexibility to choose any hardware OEM and not only the one with which the solution is being provided for future expansions.	
3.2.0	Storage scalability	The software defined storage solution should support the capability of increasing the storage capacity by simply adding another hard drive in the physical node instead of adding another physical server in the cluster	
3.3.0	Single-glass-pane-management	The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment to simplify the manageability of the entire solution	
3.4.0	Zero-data loss	The solution should provide distributed RAID and cache mirroring for intelligent placement of VM objects across disks, hosts and server racks for enhanced application availability. Zero data loss with zero downtime in case of disk, host, network or rack failure.	
3.5.0	Native in-built software based storage controller	The solution should have in-built software defined storage capability integrated within or outside the hypervisor kernel itself and should work with or without the need for any specialized dedicated controller virtual	

Srl.	Parameters	Technical Specification-SDDC for Composable IT Infrastructure	Complied (Yes/No)
		appliance.	
<b>4.0.0</b>	<b>Software Defined Networking</b>		
4.1.0	Network functions	The solution should offer to deploy virtualized network functions (like switching, routing, firewalling, VPN, DHCP and load-balancing). Administrators can build virtual networks for Virtual Machines without the need for complex VLANs, ACLs, or hardware configuration syntax on physical network.	
4.1.1		The Solution should offer Centrally managed distributed L2-L4 stateful firewall that is kernel-level integrated into the host architecture	
4.2.0	Gateway NGFW & Endpoint Protection support	The solution should be capable to provide agent based or agentless guest introspection services like Enterprise Gateway NGFW, Enterprise Endpoint Protection Software, Anti-Malware etc. and Network introspection services like IPS/IDS etc.	
4.3.0	Virtual Extensible LAN (VXLAN)	The virtual solution should offer extending Layer-2 network across multiple sites , without re-architecture or any configuration on physical network	
4.4.0	Security policy affinity	The Security policies must follow the VM in the event of migration (i.e. live migration)	
4.5.0	SD-WAN integration	Should integrate natively with SD-WAN software for ICG	
<b>5.0.0</b>	<b>SDDC - Automation and Orchestration</b>		
5.1.0	Self-service	Provide Self-service portal for Users to enable provisioning/ deprovisioning of Computer, Storage and Networking on-demand	
5.1.1		Should provide PaaS, IaaS services across IT resources on ICG DC, DR and ROBO sites	
5.2.0	Application Delivery	Automate application delivery and container management	

Srl.	Parameters	Technical Specification-SDDC for Composable IT Infrastructure	Complied (Yes/No)
5.3.0	SSO support	Should support Single-Sign-On	
5.4.0	What-if analysis	Provide What-if analysis for various Orchestration related situations	
<b>6.0.0</b>	<b>SDDC - Operations</b>		
6.1.0	DevOps support	Should support DevOps	
6.2.0	Container support	Should natively support Containers of Docker/ Kubernetes	
6.2.1		Provision/ deprovisioning of Containers in native virtualisation environment	
6.2.2		Provide HA support for Containers	
6.2.3		Provide persistent storage across Containers	
6.2.4		Support micro-segmentation for Containers	
6.2.5		Provide dedicated Container management portal integrated into SDDC main console	
6.2.6		Provide Docker image repository	
6.3.0	Performance & Capacity Monitoring Dashboard	Should provide Performance monitoring and analysis on SDDC capacity utilisation	
6.3.1		Should provide aggregated compute/ storage utilization analysis at cluster, site and enterprise level	
6.3.2		Should provide real-time predictive capacity management including trending, metering, right-sizing, optimization to achieve enhanced utilisation of IT resource	

<b>Srl.</b>	<b>Parameters</b>	<b>Technical Specification-SDDC for Composable IT Infrastructure</b>	<b>Complied (Yes/No)</b>
6.3.3		Monitoring of OS Resources including CPU, disk, memory, network etc.	
6.4.0	Overall cost view	Should provide overall cost associated with provisioned IT resources such as VM, Storage etc.	
6.5.0	What-if analysis	Provide What-if analysis for various operations related situations	
6.6.0	Application Monitoring	Should able to monitor Application, Middleware and Database for leading enterprise software systems	
6.6.1		Should natively support application monitoring for Oracle Fusion Middleware, Oracle Databased, Cisco CUCM for Enterprise Unified Communication and MS Exchange.	

Section-J – **Backup, Recovery & Replication for Business Continuity**

<b>Sl.</b>	<b>Category</b>	<b>Technical Requirements – Backup, Recovery &amp; Replication</b>	<b>Complied (Yes/No)</b>
3.1.0	<b>High Availability</b>	No Single-Point-of-Failure architecture and associated components should be provided	
3.1.1		The solution should support VM on HA configuration	
3.2.0	<b>Licensing</b>	The proposed Backup software must offer host based / CPU based licensing with no restrictions on type of arrays (protecting heterogeneous storage technologies), front end production capacity or backend backup target capacity for virtual or physical servers. Licenses and associated hardware should be supplied for DC, DR DC & ROBO as required.	
3.2.1	<b>Application awareness</b>	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, Exchange transaction logs with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.	
3.2.2	<b>Hardware Agnostic</b>	Backup software should be Hardware Agnostic software and it should support any type of storage for storing backups on disk and yet support de-duplication on the storage targets quoted. It should be able to backup data to tapes as well for long term retention.	
3.2.3	<b>Granular recovery</b>	Backup software should support file level recovery from an image level backup of Windows/Linux guest file systems.	
3.2.4		Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup (irrespective of the source size) within 15Mins RTO.	
3.2.5	<b>VM replication</b>	Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of	



Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Complied (Yes/No)
		network addresses at the destination site.	
3.2.6	<b>Unified console operation</b>	Backup software should provide Backup and Replication capabilities in one console only.	
3.2.1	<b>Encryption, WAN optimization</b>	The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured without need of any other 3rd party WAN Accelerator requirements.	
3.2.1		The proposed backup solution must support at least AES 256-bit encryption capabilities for Data-in-Rest, Data-in-Transfer support	
	<b>Tape library</b>	Should support tape mirroring of the same job running concurrently with primary backup.	
		Should allow creating tape clone facility after the backup process.	
3.2.1	<b>Recovery verification</b>	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	
3.2.1		Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.	
3.2.1	<b>API Integration</b>	Should provide RESTful API for integration with 3 <sup>rd</sup> party Enterprise applications	
3.2.1	<b>Unified management console</b>	Should provide Enterprise level unified Dashboard 'Single-pane-of-glass-monitoring and management' from central site for all ROBO units. All ROBO sites backup servers' status should be available from single unified dashboard at central site.	
3.2.1	<b>Replication on offline connectivity</b>	Should support auto ROBO replication with central site on restoration of network without any manual intervention	

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Complied (Yes/No)
3.2.1		Recovery of ROBO sites from central backup at data center should be supported with zero-touch at ROBO. Take backup of ROBO sites locally and then replicate it to central location	

Section-K – **OEM Qualification, Warranty & Implementation support**

Sl.	Category	OEM Qualification and Requirements	Complied (Yes/ No)
1.0	<b>OEM Qualification</b>	<p>(a) Data Center, DR Data Center and Zero-Touch ROBO OEM components of Hardware, Hyper-Converged Appliances for ROBO, Virtual NGFW, Backup software, SDDC software, SD-WAN should have been mentioned in latest Gartner Magic Quadrant/ Forrester Wave Reports in respective product category.</p> <p>(b) Should be registered in India and present for minimum of 05 years</p> <p>(c) Should have minimum 03 deployments of hardware/ software in Central/State Govt. Organisations in India and 05 deployments in private sector of similar size in the past 03 years.</p>	
2.0	<b>OEM implementation</b>	Design plan, implementation and validation for compute, storage, and network virtualisation to be done by OEM authorised partners having implemented minimum 03 similar projects. Undertaking for the same to be mentioned on the MAF certificate/ OEM partners should obtain ICG project specific authorization from OEM	
3.0	<b>OEM Support</b>	<p>(a) Should have OEM 24x7x365 onsite support for hardware/ software in India. Should provide Service Desk contact details and Service Level Agreement (SLA) in proof</p> <p>(b) All OEM products for ICG should have minimum of 03 years warranty from the date of delivery and acceptance of ICG</p>	

**Appendix-'C'**

*(Refer to Para-5 of RFP)*

Company letter head

[Date]

The Director General  
{for D(IT) }  
Directorate of IT, Coast Guard Headquarters  
New Delhi – 110 001

Dear Sir,

**SUB: DESIGN, DEVELOPMENT, IMPLEMENTATION AND SUPPORT FOR  
SECURE CHAT WITH SECURE APPLICATION CONTAINER (PROJECT TAPPS) -  
INDIAN COAST GUARD**

1. Refer to your RFP No.CGHQ/IT/TAPCHAT/2018-19 dated \_\_\_ Jan 2019.
2. This is to notify you that our company intends to submit a proposal for "Design, development, implementation and support for Secure Chat with Secure application container (Project TAPPS) - Indian Coast Guard".
3. Primary and Secondary contacts for our company are:

	<b>Primary Contact</b>	<b>Secondary Contact</b>
<b>Name:</b>		
<b>Title:</b>		
<b>Company Name:</b>		
<b>Address:</b>		
<b>Phone:</b>		
<b>Mobile:</b>		
<b>Fax:</b>		
<b>E-mail:</b>		

4. We confirm that the information contained in this response as per **Annexure-1 of Appendix-'C'** or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to the Indian Coast Guard is true, accurate, verifiable and complete.

Dated this Day of Jan 2019

(Signature) (In the capacity of)

Duly authorized to sign

Sincerely,

[SYSTEM INTEGRATOR'S NAME]

Name

Title

Signature

Date

(Name and Address of Company) Seal/Stamp of System Integrator

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am ..... of the ....., and that ..... who signed the above response is authorized to bind the corporation by authority of its governing body.

Date

(Seal here)

**Annexure-1 of Appendix-'C'**

*(Refer to Para-5 of RFP, Para-4 of Appendix-B)*

**CHECKLIST & INDEX OF BID**

*[Important note: All filenames of documents uploaded in e-procurement website should be numbered to match with 'Bid Page' without exception. For example: 04-technical-bid-covering-letter.pdf, 22-datasheet-datarack.pdf etc.]*

**1. RFP with enclosures**

<b>Sl.</b>	<b>Details</b>	<b>Bid Page No.</b>	<b>Check (Yes/No)</b>
<b><u>General Documents</u></b>			
(a)	Checklist & Index of Bid is attached		
(b)	Bid submission covering letter <i>(Appendix-'B')</i>		
(c)	Technical Bid with Covering letter. Covering letter &EMD to be placed inside sealed cover <i>(Appendix-'C')</i>		
(d)	RFP acknowledgement & compliance <i>(Copy of RFP duly signed on each page)</i>		
(e)	Bidder profile format included <i>(Appendix-'K')</i>		
(f)	Technical Compliance <i>(Appendix-'E')</i>		
(g)	Commercial Bid <i>(Appendix-'F')</i> with Covering letter <i>(Appendix-'E')</i> .		
(h)	(i) Technical Solution document <i>('Proposed Solution (60 Marks)' of Para-6(f) (j) in Appendix-'G')</i>  (ii) Technical Solution document for IT infrastructure <i>(Part-I of Annexure-I of Appendix-B)</i>		
(j)	Detailed Bill of Material with relevant OEM products, Supply, Services etc. & Sizing of Solution sheet. <i>(Annexure-1 of Appendix-'H'-Commercial Bid Format)</i>		
(k)	POC of Secure Chat demo project document included <i>(Annexure-1 of Appendix-'J')</i>		
(l)	POC demo app for Secure Application Container and project document included <i>(Annexure-2 of Appendix-'J')</i>		

Sl.	Details	Bid Page No.	Check (Yes/No)
(q)	MAF Certificate from OEM for Secure Application Container, Composable IT infrastructure Server, SAN Switch, Rack Server, Tape Library, Virtual NGFW with WAF and Private Cloud Virtualisation Software etc.		

2. **Technical Brochures/ Data Sheets/ Manuals**

Sl.	Technical Brochures/ Data Sheets/ Manuals	Bid Page No.	Check (Yes/No)
(a)	Brochure & Datasheet of Secure Chat software		
(b)	Brochure & Datasheet of Secure Application Container software		
(c)	Brochure & Datasheet of IT infrastructure including Composable IT Infra, Rack Servers, SAN Switch and Tape library		
(d)	Brochure & Datasheet of Virtual NGFW and WAF		
(e)	Brochure & Datasheet of Private Cloud Virtualisation Software		
(f)	Brochure & Datasheet for Backup, recovery and replication Software		

3. **List of Enclosures**

Sl.	Appendix Description	Bid Page No.	Check (Yes/No)
(a)	Technical Offer with EMD, if applicable(In separate sealed cover)		
(b)	Detailed breakdown of Bill of Material/ Services (Annexure-I to Appendix-H)		

**Note:**

(a) The check list as above is to be fully completed and enclosed along with the bid covering letter along with technical bid.

(b) The technical bid shall, additionally, consist of the following documents in the sequence given below: -

(i) Index page indicating the technical bid contents with appropriate page numbers.

(ii) Deviations, assumption and exclusions from Scope of Work.

(c) In case necessary documentary proofs are not enclosed the firm would be rejected during Technical Evaluation.

Signature with date & Stamp of Firm

**Appendix-'D'**

**Covering letter format for Technical Bid**

(Company letterhead) [Date]

To

The Director General  
{for D(IT) }  
Directorate of IT, Coast Guard Headquarters  
New Delhi-110 001

Dear Sir,

**SUB: DESIGN, DEVELOPMENT, IMPLEMENTATION AND SUPPORT FOR  
SECURE CHAT WITH SECURE APPLICATION CONTAINER (PROJECT TAPPS) -  
INDIAN COAST GUARD**

1. Refer to your RFP No. CGHQ/IT/TAPPS/2018-19 dated \_\_\_ Jan 2019.
2. Having examined the bid document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer for "Design, development, implementation and support for Secure Chat with Secure Application Container (project TAPPS) - Indian Coast Guard" as required and outlined in the RFP for Indian Coast Guard. To meet such requirements and provide such services as required are set out in the bid document.
3. We attach hereto the bid technical response as required by the bid document as per format in **Appendix-'D'**, which constitutes our proposal. We undertake, if our proposal is accepted, to provide all the functional and non-functional requirements of the solution put forward in Part II of the RFP or such features as may subsequently be mutually agreed between us and Indian Coast Guard or its appointed representatives. We agree for unconditional acceptance of all the terms and conditions set out in the bid document and also agree to abide by this bid response for a period of SIX (06) MONTHS from the date of submission of bids and it shall be a valid proposal till such period with full force and virtue. Until within this period a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and Indian Coast Guard.
4. We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules and other documents and instruments delivered or to be delivered to Indian Coast Guard is true, accurate and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead Indian Coast Guard as to any material fact.





**Appendix-'E'**  
(Refer to Para-3 of Appendix-D)

### **TECHNICAL COMPLIANCE SHEET**

(Note: Vendor to upload duly ink-signed copy of RFP alongwith technical compliance sheet. Details of following RFP clauses as per RFP issued by this Office)

Sl.	RFP Clause	RFP Requirement	Compliance (Yes/No), deviations if any
<b>01.</b>	<b>RFP Covering letter, Para-1 to 7</b>	Covering letter for RFP No.CGHQ/IT/TAPPS/2018-19 dated ___ Jan 2019of Coast Guard Headquarters, New Delhi	
<b>02.</b>	<b>Part-I of Encl.-I:- General Information</b>		
(a)	Para-1	Last date and time for depositing the Bids	
(b)	Para-2	Manner of depositing the Bids	
(c)	Para-3	Time and date for opening of Bids	
(d)	Para-4	Address of Submission of EMD	
(e)	Para-5	Place of opening of the Bids: [DIT,CGHQ, New Delhi]	
(f)	Para-6	Two-Bid system	
(g)	Para-7	Forwarding of bids	
(h)	Para-8	Clarification regarding contents of the RFP	
(j)	Para-9	Modification and Withdrawal of bids	
(k)	Para-10	Clarification regarding contents of the bids	
(l)	Para-11	Rejection of Bids	
(m)	Para-12	Unwillingness to Quote	
(n)	Para-13	Validity of Bids	
(p)	Para-14	Earnest Money Deposit	
<b>03.</b>	<b>Part II – Essential Details of Items/Services required</b>		
(a)	Para-1	Schedule of Requirements.	
(b)	Para-2	Technical Details. Detailed compliance submitted as per <b>Appendix-'A'</b> .	
(c)	Para-3	Two bid system	
(d)	Para-4	Delivery Period	
(e)	Para-5	INCOTERMS for Delivery and Transportation	
(f)	Para-5	Consignee Details	
<b>04.</b>	<b>Part III – Standard Conditions</b>		
(a)	Para-1	Law	
(b)	Para-2	Effective Date of the Contract	

<b>Sl.</b>	<b>RFP Clause</b>	<b>RFP Requirement</b>	<b>Compliance (Yes/No), deviations if any</b>
(c)	Para-3	Arbitration	
(d)	Para-4	Penalty for use of Undue influence	
(e)	Para-5	Agents / Agency Commission	
(f)	Para-6	Access to Books of Accounts	
(g)	Para-7	Non-disclosure of Contract documents	
(h)	Para-8	Liquidated Damages	
(j)	Para-9	Termination of Contract	
(k)	Para-10	Notices	
(l)	Para-11	Transfer and Sub-letting	
(m)	Para-12	Patents and other Industrial Property Rights	
(n)	Para-13	Amendments	
(p)	Para-14	Taxes and Duties	
(q)	Para-15	Pre-Integrity Pact Clause	
<b>05.</b>	<b>Part IV – Special Conditions</b>		
(a)	Para-1	Performance Guarantee	
(b)	Para-2	Option Clause	
(c)	Para-3	Repeat Order Clause	
(d)	Para-4	Tolerance Clause	
(e)	Para-5	Payment Terms for Indigenous Sellers	
(f)	Para-6	Payment terms for Foreign Sellers	
(g)	Para-7	Advance Payments	
(h)	Para-8	Paying Authority	
(j)	Para-9	Fall clause	
(k)	Para-10	Exchange Rate Variation Clause	
(l)	Para-11	Risk & Expense clause	
(m)	Para-12	Force Majeure clause	
(n)	Para-13	Buy-Back offer	
(p)	Para-14	Specification	
(q)	Para-15	OEM Certificate	
(r)	Para-16	Export License	
(s)	Para-17	Earliest Acceptable Year of Manufacture	
(t)	Para-18	Buyer Furnished Equipment	
(u)	Para-19	Transportation	
(v)	Para-20	Air lift	
(w)	Para-21	Packing and Marking	
(x)	Para-22	Quality	
(y)	Para-23	Quality Assurance	

<b>Sl.</b>	<b>RFP Clause</b>	<b>RFP Requirement</b>	<b>Compliance (Yes/No), deviations if any</b>
(z)	Para-24	Inspection Authority	
(aa)	Para-25	Pre-Dispatch Inspection	
(ab)	Para-26	Joint Receipt Inspection	
(ac)	Para-27	Franking clause	
(ad)	Para-28	Claims	
(ae)	Para-29	Warranty	
(af)	Para-30	Product Support	
(ag)	Para-31	AMC Clause	
(ah)	Para-32	ESP Clause	
(aj)	Para-33	PV Clause	
<b>06.</b>	<b>Part V – Evaluation Criteria &amp; Price Bid issues</b>		
(a)	Para-1	Evaluation Criteria	
(b)	Para-2	Price Bid Format	

**Annexure-I to Appendix-'E'**  
(Refer to Para-3(a)&(b) of Appendix-'E')

**SCHEDULE OF REQUIREMENT & TECHNICAL SPECIFICATION COMPLIANCE**

<b>SL.</b>	<b>QR Requirement</b>	<b>QR Specification</b>	<b>Compliance (Yes/ No). Deviations, if any.</b>
01.	Schedule of Requirements <i>(Para-1(a), Part-II of RFP)</i>	<p>(a) Design, development, implementation and support for <b>Secure Chat with Secure application container (Project TAPPS)</b> based on proven software including supply of Secure application container (Unified Endpoint Management-UEM) software licenses and private cloud IT infrastructure with hardware/ software as required. Project to <b>be implemented on turn-key basis</b> and vendor to include all required hardware/ software as required. Selection of Bidder shall be based on QCBS method as elaborated in <b>Appendix-'J'</b>.</p> <p>(b) Information security audit of complete implementation including Secure Chat software and other IT infrastructure by CERT-IN empaneled vendor</p> <p>(c) Secure Chat Software Warranty for 01 year from final GoLive and 02 year All Inclusive Annual Maintenance Support (AIAMC) including onsite manpower support. Other OEM hardware/ software to be supplied with 03 year warranty with 24x7 support.</p>	
02.	Vendor Pre-qualification Requirement <i>(Para-1(e), Part-II of RFP)</i>	<p>(i) <u>Package-A:</u> <b>Secure Chat software application:</b> Design, development, implementation and support for Secure Chat application for ICG (Package-A of Para-1(d))</p> <p>(ii) <u>Package-B:</u> <b>Supply, implementation of Secure Application Container:</b> Supply of software licenses - 10,000 Nos. and <b>IT</b></p>	

SL.	QR Requirement	QR Specification	Compliance (Yes/ No). Deviations, if any.
		<p><b>infrastructure to host Secure Chat application at ICG Data Center:</b> Supply, deployment and support of Enterprise grade Private Cloud IT infrastructure along with necessary support (Package-B of Para-1(d))</p>	
03.	<p>Technical Specifications <i>(Para-2, Part-II of RFP)</i></p>	<p>Design, configuration, customization, development, implementation and support for Secure Chat with Secure Application Container includes following.</p> <p>(i) <b>Secure Chat software application:</b> Design, development, implementation and support for Secure Chat software</p> <p>(ii) <b>Supply, implementation of Secure Application Container:</b> Supply of software licenses - 10,000 Nos. (iii) <b>IT infrastructure to host Secure Chat application at ICG Data Center:</b> Supply, deployment and support of Enterprise grade Private Cloud IT infrastructure along with necessary support</p> <p>(iii) <b>Security Audit</b> by entire system including Secure Chat software and related IT infrastructure to be security audited by <b>CERT-IN empaneled vendor</b> on go-live and during warranty/support as required by ICG</p> <p>(iv) Details of Functional Requirement and Non-Functional Requirements as per <b>Appendix-A, Appendix-B of RFP</b> respectively</p>	

**Covering letter format for Commercial Bid.**

Company letter head

[Date]

The Director General  
{for D(IT) }  
Directorate of IT, Coast Guard Headquarters  
New Delhi – 110 001

Dear Sir,

**SUB: DESIGN, DEVELOPMENT, IMPLEMENTATION AND SUPPORT FOR  
SECURE CHAT WITH SECURE APPLICATION CONTAINER (PROJECT TAPPS) -  
INDIAN COAST GUARD**

1. Refer to your RFP No. CGHQ/IT/TAPPS/2018-19 dated \_\_\_ Jan 2019.
2. Having examined the bid document, the receipt of which is hereby duly acknowledged, we, the undersigned, offer for "Design, development, implementation and support for Secure Chat with Secure Application Container (project TAPPS) - Indian Coast Guard" as required and outlined in the RFP for Indian Coast Guard. To meet such requirements and provide such services as required are set out in the bid document.
3. We attach hereto the bid \_\_\_\_\_ of commercial response as required by the bid document, which constitutes our proposal. We undertake, if our proposal is accepted, to provide all the functional and non-functional requirements of the solution put forward in Part II of the RFP or such features as may subsequently be mutually agreed between us and Indian Coast Guard or its appointed representatives. We agree for unconditional acceptance of all the terms and conditions set out in the bid document and also agree to abide by this bid response for a period of SIX (06) MONTHS from the date of submission of bids and it shall be a valid proposal till such period with full force and virtue. Until it is in this period a formal contract is prepared and executed, this bid response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and Indian Coast Guard.
4. We confirm that the information contained in this proposal or any part thereof, including its exhibits, schedules and other documents and instruments delivered or to be delivered to Indian Coast Guard is true, accurate and complete. This proposal includes all information necessary to ensure that the statements therein do not in whole or in part mislead Indian Coast Guard as to any material fact.

5.

We agree that you are not bound to accept the lowest or any bid response you may receive. We also agree that you reserve the right in absolute sense to reject all or any of the products/services specified in the bid response without assigning any reason whatsoever.

6. The soft-

copies of the proposals submitted by us and the related addendums and other documents including the changes made to the original tender documents issued by Indian Coast Guard, conform to and are identical with the hard-copies of aforesaid proposal submitted by us, in all respects.

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

Dated this Day of **Jan 2019**

(Signature) (In the capacity of)

Duly authorized to sign the Bid Response for and on behalf of: (Name and Address of Company) Seal/Stamp of SI

**CERTIFICATE AS TO AUTHORISED SIGNATORIES**

I, certify that I am ..... of the ..... and that ..... who signed the above Bid is authorized to bind the company, pursuant to the resolution passed in the meeting of Board of Directors of the company \_\_\_\_\_ (date).

Date

**(Seal here)**

**Encl:** Commercial Bid as per **Appendix-'F'** of RFP

**Appendix-'G'**  
(Refer to Para-2, Part-V of RFP)

**COMMERCIAL-BID FORMAT**

*Note: Bidder to submit commercial bid on-line only. However, Annexure-1 of Appendix-'H' need to be submitted in sealed cover separately.*

**1. Item/ service bill of material**

Item ID	Description	Qty.	Unit	Make & Model	Unit Price(Rs)	Total w/o Tax	GST (%)	GST (Rs.)	Total with tax
	<b>(A) SECURE CHAT SOFTWARE DEVELOPMENT</b>								
A-01	Design, Development, Configuration, Installation, Testing, system integration and Commissioning including 01 year warranty with one onsite support engineer	1	No.						
	<b>(B) SECURE UNIFIED ENDPOINT MANAGEMENT (UEM) SOFTWARE</b>								
B-01	Unified Endpoint Management software with 03 years warranty support	10000	No.						
	<b>(C) IT INFRASTRUCTURE FOR ICG PRIVATE CLOUD, 03 YEARS WARRANTY</b>								
C-01	Composable IT Infrastructure Server Hardware	1	No.						
C-02	Tape Library	1	No.						
C-03	Rack Server	2	No.						
C-04	SAN Switch	2	No.						
C-05	Virtual NGFW with WAF	2	No.						
C-06	Private Cloud Virtualisation Software, 04 CPU	1	Set						



Item ID	Description	Qty.	Unit	Make & Model	Unit Price(Rs)	Total w/o Tax	GST (%)	GST (Rs.)	Total with tax
C-07	Backup, recovery and Replication Software, 04 CPU	1	No.						
	<b>(D) INSTALLATION, SUPPORT &amp; MAINTENANCE, 01 YEAR WARRANTY</b>								
D-01	Installation, Customisation, Configuration, Installation, Testing, system integration and Commissioning of IT infrastructure, Secure Application Container including 01 year warranty	1	No.						
	<b>(E) AIAMC FOR SUPPORT &amp; MAINTENANCE, RECURRING</b>								
E-01	Secure Chat software, AMC for 01 year, Support includes 01 onsite engineer, minor feature enhancements, bugs, ticketing system, performance management and routine patches	2	Yrs						
	<b>Grant Total</b>								

**(Grant total is, Rupees \_\_\_\_\_ only excluding taxes)**

**(Grant total is, Rupees \_\_\_\_\_ only including taxes)**

**Note:**

(a) **L1 shall be decided on QCBS basis (exclusive of taxes) as single package.**

(b) Individual taxes need to be added as separate columns

(c) Taxes mentioned in the format are indicative only, and vendor need to mention taxes as applicable at the time of bidding

- (d) Training is conducted at New Delhi for 25- 30 candidates
- (e) Provide detailed line item for each 'Item ID' as required by the Coast Guard as per Annexure-1 of Appendix-H
- (f) To qualify as COTS software, product should have 10 years of maturity, atleast 03 certified support partners in India each having atleast 02 current client each with minimum of Rs.2 Crore product value, product having atleast 25 current deployments, product to have dedicated support portal with datasheets/user manuals/ API manuals/admin manuals/ patches and published roadmap for next 05 years
- (g) Warranty of software implementation should commence from final GoLive with acceptance of Coast Guard
- (h) Detailed sizing and technical specifications as per **Annexure-i, Appendix-B of RFP.**

**Annexure-1 to Appendix-'G'**

**Detailed breakdown Bill of Material/Services**  
*(To be submitted in sealed cover separately)*

Sl.	Item ID	Detailed Description of OEM items	Qty.	Unit	Make & Model with Part No.	Unit Price(Rs)	Total w/o Tax	GST	Total with Tax	Total
1	A-01		1	No.						
2	A-01		1	No.						
3	A-03	<i>(Any other items as required)</i>	0	No.	<i>Make as applicable</i>					

**Note:-**

- (a) 'Item ID' as per para-1 of Appendix-'H'
- (b) Line item should be as per OEM description along with respective 'Part No/ Code'
- (c) Sealed cover for Annexure-1 to Appendix-'H' to be handed-over to the Buyer as part on online bid submission. However, in case of discrepancies in price, online bid prices shall be considered as actual.

**CAMPUS SECURE LAN-62 :PRE-QUALIFICATION POC TESTS**  
**COMPOSABLE IT INFRASTRUCTURE**

Test ID	Category	POC Description – Composable IT Infrastructure	Qualified (Yes/No)
<b>General</b>			
01-00	<b>Composable IT infrastructure technical solution document</b> <i>(Should be submitted as part of Technical bid)</i>	As per Annexure-1 of Appendix-'H'	
02-00	<b>POC Setup</b> <i>(Carry out as part of Technical Evaluation)</i>	(i) Centralised monitoring software (a) 03 Server node instance (b) Centralised SDDC to provide Enterprise level unified 'Single-pane-of-glass' dashboard at central site  (ii) Physical Server (a) Setup with 03 Server nodes (b) Centralised cloud setup with 'Single-pane-of-glass' dashboard at central site  (iii) Backup & Recovery (a) Setup for 03 Server instances with backup software (b) Centralised Cloud Management console integrated with Backup software setup with 'Single-pane-of-glass' dashboard at central site  (iv) Virtual Next Generation Firewall (a) Setup for 03 Server node instances with NGFW software and WAF (b) Centralised HCI/ HCA with NGFW software setup with 'Single-pane-of-glass' dashboard at central	

Test ID	Category	POC Description – Composable IT Infrastructure	Qualified (Yes/No)
		site	
03-00	Presentation	Overall solution presentation to include layout diagram, sizing/bill of material and project plan	
04-00	Layout diagram	2D layout diagram of Composable IT infrastructure Cloud data-rack, depicting electrical, networking, data rack layout	
05-00	Sizing & Bill of Material list	(i) Sizing of entire solution including Composable IT Infrastructure, Cloud virtualization with SD-NGFW/ Backup & Recovery software, ALB Software (ii) Bill of Material with Make & Model, Quantity	
06-00	Project Plan	(i) Delivery timeline for Composable IT Infrastructure (ii) Delivery timeline for software (iii) Gantt chart based project timeline	
07-00	Composable IT Infrastructure	POC setup made available as per ICG requirement	
07-01	Fluid resource pool	Compute, storage and networking resources should be fluid, separated from underlying physical infrastructure and independent of each other	
07-02		Support heterogeneous platforms that includeESXi, Hyper-V , Oracle VM Server, Linux KVM, Openstack hypervisors and next generation containers and Bare metal servers concurrently on the same cluster	
07-03		Should provide unified single GUI to manage fluid resource pool	
07-04		Enables automation-based user self-service, and provide 'Private Cloud' services	

Test ID	Category	POC Description – Composable IT Infrastructure	Qualified (Yes/No)
07-05		Allows an application to automatically instantiate new infrastructure based on performance conditions at the present time	
07-06		Enables developers to programmatically deploy new virtual machines	
08-00	Single-pane-of-glass monitoring	SDDC software of Composable IT infrastructure configured and display all 03 Server nodes instances aggregated into single unified dashboard.	
08-01		Cloud virtualisation software of Composable IT Infrastructure configured and display all 03 Server node instances aggregated into single unified dashboard	
08-02		Virtual NGFW software of Composable IT Infrastructure configured and display all 03 Server node instances aggregated into single unified dashboard	
08-03		Backup and recovery software of Composable IT Infrastructure configured and display all 03 Server node instances aggregated into single unified dashboard	
09-00	WAN optimised, Cloud central monitoring systems	Should support network environment consists of no network connectivity, 64Kbps VSAT high-latency connectivity, 2 Mbps to 8 Mbps	
09-01		SDDC software should able to function within allotted WAN bandwidth and at predefined duration defined as custom WAN profile. For example, for Site-X, allotted maximum allotted bandwidth for SDDC software is 64 Kbps and only communicate during off-hours it mid-night 00:00 hrs to 04:00 hrs.	
09-02		Should support off-line no network environment such as remote islands and ICG ships. On availability/ restoration of network connectivity should sync with central servers subject to custom WAN profile.	

Test ID	Category	POC Description – Composable IT Infrastructure	Qualified (Yes/No)
10-00	Central policy defining, and applying from central location	Cloud virtualisation software of Composable IT Infrastructure configured for central policy & enforcement dynamically for all 03 Server node instances from central location	
10-01		Virtual NGFW software of Composable IT Infrastructure configured for central policy & enforcement dynamically for all 03 Server node instances from central location	
11-00	Survivability	Provide live demo on Cloud virtualisation for Software Defined Computer, Storage & Networking to exhibit High-Availability (HA) within Site to provide both RTO & RPO to 15 minutes	
12-00	Disaster Recovery using backup software	Site Recovery (SR) to provide RTO & RPO of not exceeding 12 Hrs and automated Recovery Testing scenario of VMs to other remote site	
13-00	Test recovery using backup software	Able to test backup & recovery on sandboxed network environment of having different subnet IP. Backup should be recovered for testing from production backup on disk	
14-01		App aware test recovery of MS Exchange. It is required to test disaster recovery drill at regular intervals without affecting production environment	
15-00	Backup software	Carryout demo backup & recovery of VM images, blocks and files	
16-00	Backup software for app aware	Carryout app aware backup & recovery of MS Exchange test deployment and recover granular data such as individual email and mail box	

**Annexure-1 of Appendix-'H'**  
*(Para-01-00 of Appendix-'H')*

**POC Demo for Composable IT Infrastructure**

*Note:*

*(a) Bidder should provide demo POC project documentation in following format as part of Technical Bid. Subsequently should provide live demo and MS PowerPoint presentation to Coast Guard Technical Evaluation Committee (TEC))*

Template format for POC Project Document. The Bidder should prepare document in following structure

**Part-A: Introduction**

- 1.0: Title of POC demo project
- 2.0: Index
- 3.0: Executive Brief (Should be within single A4 size page)
- 4.0: User Requirement
- 4.1: Solution architecture diagram
- 4.2: Bill of material & purpose of each item

**Part-B: Design &Deployment architecture**

- 5.0: Solution sizing including power/ heat calculation
- 5.1: Overall deployment architecture of Composable IT infrastructure
- 5.2: Deployment architecture of SDDC software and Centralised management console sample screen depicting all 03 Server nodes in unified Dashboard

**Part-D: Project Planning**

- 6.0: Project planning & monitoring
  - (a) Include Work Breakdown Structure (WBS), Resource Allocation etc using MS Project/ Oracle Primavera
  - (b) Overall timeline

**Part-E: Deployment at site**

- 7.0: Sample Site diagram and area of responsibility for Vendor and Coast Guard
- 7.1: Scope of work for Vendor



7.2: Centralized Server enclosure monitoring integration

**Part-F: Live POC Demo setup**

8.0: Documentation of POC demo setup architecture layout, objective, test cases

**Part-G: Documentation** and presentation

9.0: Documentation and quality of presentation shall be evaluated based on compliance to Datacenter standards, Business Continuity standards, Safety standards diagrams etc.

**Appendix-'J'**

(Refer to Para-1(a) of Part-II of RFP  
, Para-1(a) of Part-IV of RFP)

**TECHNICAL/COMMERCIAL EVALUATION FRAMEWORK**  
**(QUALITY & COST BASED SELECTION)**

**Introduction.**

1. Secure Chat application need to be made available on reliable basis for Coast Guard and hence Coast Guard intend to qualify vendors having strong experience in implementing similar projects and Secure Chat products qualifying to meet challenging conditions of Coast Guard.

**Evaluation of Quotation:**

**2. Technical Evaluation: -**

(a) Each Technical bid will be assigned a technical score out of a maximum of **400 marks** (marks breakup described in **Appendix-'G'**). Only the bidders who get a technical score of **50 percent or more** in each section and **60 percent or more** overall will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the bid.

(b) The normalized technical score of the bidder shall be calculated as follows:

**Normalized Technical Score of a bidder = {Technical Score of that bidder / Score of the bidder with the highest technical score} X 400 (adjusted to 2 decimals)**

**(c) Final score calculation through QCBS (Quality and Cost based selection)**

Example: Technical Score

Bidders	Technical score (B)	Normalized Technical score	Final Score
1	350	$(350/390)*400$	358.97
2	360	$(360/390)*400$	369.23
3	370	$(370/390)*400$	379.49
4	380	$(380/390)*400$	389.74

Bidders	Technical score (B)	Normalized Technical score	Final Score
5	390	$(390/390)*400$	400

3. **Commercial Evaluation:** -

(a) Technically qualified bidders as per technical evaluation process will participate in commercial bid opening process. The bidder with the lowest commercials as per Price Formats provided by ICG(**as uploaded in e-procure website**) will be declared commercially L1 bidder and further evaluated as per following method:

(b) Normalized Commercial Score of a bidder = {lowest quote/ bidders quote} X 400 (adjusted to 2 decimals)

Example: Commercial Score

Bidders	Price Quoted by bidders (in Lakhs)	Normalized commercial score	Final Score
1	10	$(10/10)*400$	400
2	11	$(10/11)*400$	363.64
3	12	$(10/12)*400$	333.33
4	13	$(10/13)*400$	307.61
5	14	$(10/14)*400$	285.71

4. **Final score calculation through QCBS**

(a) The final score will be calculated through Quality and Cost based selection method with the following weightage:-

**Technical: 70% Commercial: 30%**

(b) Final Score = (0.70\*Normalized Technical Score) + (0.30\*Normalized Commercial Score)

Bidders	Final Technical score	Final Commercial score	Final Score (70:30)
<b>1</b>	<b><math>358.97*.7</math></b>	<b><math>400*.3</math></b>	<b>371.28</b>
2	$369.23*.7$	$363.64*.3$	367.55
3	$379.49*.7$	$333.33*.3$	365.64
4	$389.74*.7$	$307.61*.3$	365.13

Bidders	Final Technical score	Final Commercial score	Final Score (70:30)
5	400*.7	285.71*.3	365.71

(c) The bids with Highest Final Score will be selected.

## 5. **Technical Evaluation Framework**

(a) The bidder's technical solution proposed in the technical evaluation bid document will be evaluated as per the evaluation criteria mentioned in the table below:

#	Evaluation Criteria	Total Marks	Minimum Qualifying Marks (Cut-off)
(i)	Proposed Secure Chat Product, COTS	80	>=40 (50%)
(ii)	Bidder's Experience	50	>=25 (50%)
(iii)	Bidder Employee Strength	50	>=25 (50%)
(iv)	Certification	20	>=10 (50%)
(v)	Secure Chat Demo	60	>=30 (50%)
(vi)	Proposed Solution	90	>=45 (50%)
(vii)	Software Development Demo	50	>=25 (50%)
	<b>Total</b>	<b>400</b>	<b>&gt;= 240 (60%)</b>

(b) The Buyer reserves the right to check/validate the authenticity of the information provided in the pre-qualification and Technical evaluation criteria and requisite support must be provided by the bidder.

6. The following sections explain how the bidders will be evaluated on technical evaluation criteria.

Sl.	Criteria	Details	Documentary Evidence	Max. Marks
		<b>Proposed Secure Chat Product, COTS (80 Marks)</b>		
(a)	Acceptability of proposed Secure Chat Product (COTS/Non-COTS)	(i) The proposed Secure Chat solution is expected to have minimum of 01 active implementations with One-to-One Chat, One-to-Group Chat features: - >=05 active implementations - 50 Marks >=01 active implementations - 40	Work Order/ Purchase Order supported by Customer Completion / Product Acceptance Certificate/Self Certification by OEM/	80

Sl.	Criteria	Details	Documentary Evidence	Max. Marks
		<p>Marks</p> <ul style="list-style-type: none"> <li>* 20 additional marks if 05 of the implementation is from Central/State Government departments/public sector units</li> <li>* 10 additional marks if one of the implementation is from Armed Forces/Defence PSU departments of India/Abroad</li> </ul>	<p>Documentary Proof/ Reference letter from customers stating modules implemented and active users</p>	
		<p><b>Bidder's Experience of Enterprise Software implementation (50 Marks)</b></p>		
(b)	<p>Bidder Experience in Software Implementation</p>	<p><b>Prior Experience:</b> Active software applications in India for last 5 years:</p> <ul style="list-style-type: none"> <li>* At least one (01) citation should be completed/ progress, and should cover similar projects development environment scope in single work order</li> <li>* 05 citations of successfully completed) = 40</li> <li>* 03 citations of successfully completed) = 30,</li> <li>* 01 citations of successfully completed/ progress) = 20</li> <li>* 10 additional marks if 01 of the citations is from Central Govt./ Central Public Sector Unit</li> </ul>	<p>Copy of work order + Completion/Progress Certificates from the client; (OR) Work Order + Self Certificate of Completion (Certified by CS/independent auditor of the bidding entity);</p>	<p>50</p>
		<p><b>Bidder Employee Strength of Secure Chat Development(50 Marks)</b></p>		
(c)	<p>Bidder Employee Strength</p>	<p>The Bidder is expected to have:</p> <ul style="list-style-type: none"> <li>(i) 50 technically qualified professionals in the area of solution architecture, software implementation including J2EE, Middleware, software development, systems integration, functional subject matter experts (SME). Qualified Payroll SME in should be minimum of 02 Nos. with OEM Certification on SME subject with 03 years' experience and 01 certified software professionals on Middleware platform.</li> <li>(ii) 04 out of the above Software</li> </ul>	<p>Self-declaration on company letter head signed by authorized signatory + Resume of key resources. If considering third party experts, include authorization from the employing party. If</p>	<p>50</p>

Sl.	Criteria	Details	Documentary Evidence	Max. Marks
		<p>experts (Reference certificates to be provided from clients in India/ Self-certification) should have experience on the bidder's offered implementation model (public cloud/private cloud/hybrid) of proposed Secure Chat on company's payroll.</p> <p>Marks for the experience shall be awarded as under: -</p> <p>* If on-roll at least 75 qualified professionals as per (i) above, 05 J2EE/Java certified and 03 OEM Middleware Certified SME = 30</p> <p>* If on-roll at least 50 qualified professionals as per (i) above 05 J2EE/Java certified and 03 OEM Middleware Certified SME = 20</p> <p>*-----*</p> <p>* at least <math>\geq 05</math> and <math>&lt; 10</math> qualified J2EE/ Middleware professionals as per (ii) above = 05</p> <p>* <math>\geq 10</math> qualified J2EE/ Middleware professionals qualifying as per (ii) above = 10</p> <p>* 10 additional marks for at least 03 Software Development professionals qualifying as per (ii) in Central/State Govt. projects.</p>	<p>considering consulting service support from OEM, include citation of support from OEM.</p>	
		<p><b>Prime Bidder Certification (20 Marks)</b></p>		
(d)	<p>Certification</p>	<p>The Bidder is expected to have at least ISO 9001:2008 or latest certification – 10 Marks</p> <p>* 10 additional marks will be awarded if the Bidder also has any 2 of the following additional certifications.</p> <ul style="list-style-type: none"> <li>- ISO 27001:2013 or latest</li> <li>- ISO 20000 or latest</li> <li>- CMMi-3/CMMi 5</li> </ul>	<p>Valid copy of certificate</p>	<p>20</p>
		<p><b>POC of Secure Chat app (80 Marks)</b></p>		
(e)	<p>Software project planning &amp;</p>	<p>The Bidder should provide demo Payroll application &amp; should display all</p>	<p>Attach POC demo project documentation</p>	<p>80</p>

Sl.	Criteria	Details	Documentary Evidence	Max. Marks
	design expertise	of required features	and to provide POC during TEC as per <b>Annexure-1 of Appendix-'J'</b> format	
		<b>Proposed Solution (60 Marks)</b>		
(f)	Proposed Solution Document	<p>The Bidder submits a detailed implementation plan for the project, with clear milestones.</p> <p>The bidder is expected to define execution methodology, and how incremental development can be made operational.</p> <p>Evaluation shall be done based on how efficiently implementation window is planned</p>	Documentation of proposed solution including sizing, architecture, integration, project plan. Document to be submitted as part of Technical Bid.	10
(g)	Solution-Architecture	<p>Functional architecture, Application architecture, Integration architecture, &amp; Infrastructure deployment architecture proposed, Project Plan and presentation covering at minimum the below key aspects:</p> <p>(i) Modularity of the system</p> <p>(ii) Scalability to handle future load by adding additional compute and no constraints on the application</p> <p>(iii) Suitability of Tools &amp; Technologies proposed including capacity to handle large transactional load</p> <p>(iv) Approach for handling frequent changes to Workflows/Rules/Organization Structures/Policies</p> <p>(v) Approach for making runtime changes, new reports/dashboards</p> <p>(vi) Cross browser compatibility - mention cross browser testing results, if available</p> <p>(vii) Risk and mitigation Plan</p> <p>(viii) Single sign on with ICG domain Marking will be based on evaluation of design/architecture</p>	<ul style="list-style-type: none"> <li>- Presentation of Solution/ Demo</li> <li>- Bill of Material</li> <li>- Illustrations supporting solution's capability in area of scaling, modularity, load, business configurations, etc.</li> <li>- OEM Certified Brochure/Data Sheet/Product Manual</li> </ul>	20

Sl.	Criteria	Details	Documentary Evidence	Max. Marks
		aspects by ICG (ix) Project plan in MS Project/ Oracle Primavera		
(h)	Solution- Multi Channel Delivery	The solution shall be capable of delivering multi-channel delivery in terms of mobility, desktop. (i) Responsive UI with menu/forms/UI out-of-box optimized for display on mobile/tablet/laptop/desktop without any distortion or loss of usability	Proposal and presentation OEM Certified Brochure/Data Sheet/Product Manual	10
(j)	Solution - Information Security	The proposal shall clearly state approach for security while: (i) Integrating with ICG domain/LDAP/AD for SSO (ii) Security architecture deployed for transactional data (iii) Native security features of Oracle database such as Data vault, Label security, Advanced Data Encryption etc. (iv) Integration with SIEM (v) Integrate with ICG Oracle Identity and Access Management (IAM)/ Equivalent IAM	Proposal document and presentation	20
		<b>Demo of Secure Application Container Software (60 Marks)</b>		
(k)	Project Development Demo	Demo of the sample environment on variety of applications, endpoints to the TEC members. One-hour demo to showcase the following: - (i) Demo of Android/ iOS publishing, lifecycle management including publish of latest upgrade patches (ii) Secure Chat deployment and integration to showcase Mobile Application Management (MAM) capabilities (iii) Various security features on mobile phone	Demo to TEC of Coast Guard. Provide demo POC project document and presentation as per <b>Annexure-2 of Appendix-'J'</b>	60
				<b>400</b>





**Annexure-1 of Appendix-'J'**

**Technical QCBS - demo of Secure Chat application**

*Note:*

(a) *Sample demo application of Bidders' existing Payroll ERP software application as POC. Bidder need to exhibit required software engineering expertise and healthcare information system expertise to ICG Technical Evaluation Committee (TEC).*

(i) *Secure Chat App. Bidder to demonstrate sample of 100 Users environment to bring out important Secure Chat features to TEC.*

**POC Project Document** (Refer. Para-6(e) of Appendix-'G' of RFP). The Bidder should prepare document and submit Part-A as part of Technical Bid in following structure and provide detailed demo of Part-B during TEC

**Part-A: Project Document for POC** (20 Marks) [To be submitted with Technical Bid]

1.0: Title of POC demo project

2.0: Index

3.0: Executive Brief (Should be within single A4 size page)

4.0: User Requirement

4.1: Storyboard of sample secure chat episode to cover all POC modules

4.2: Use Cases for 4.1

4.2: Screenshots, description of each Use Case as per 4.2

**Part-B: POC Demonstration** (60 Marks) during POC to TEC

		<b>Marks</b>	<b>Scored</b>	<b>Qualified [Y/N] (<math>\geq 50\%</math>)</b>	
<b>1.0:</b>	<b>One-to-One</b>	<b>10</b>			Para-6(e) of Appendix-'G'
1.1:	Send One-to-One Text Message	05			
1.2	Send One-to-One PDF document Send evaporated message	05			

		<b>Marks</b>	<b>Scored</b>	<b>Qualified [Y/N] (<math>\geq 50\%</math>)</b>	
<b>2.0</b>	<b>One-to-Group</b>	<b>10</b>			
2.1	Send One-to-Group Text Message				
	Send One-to-Group PDF document				
<b>3.0</b>	<b>Voice/ Video Call</b>	<b>10</b>			
3.1	Make Voice Call	05			
3.2	Make Video Call	05			
<b>4.0</b>	<b>Security</b>	<b>10</b>			
4.1	Send evaporate message	05			
4.2	Send message with security pin	05			
<b>5.0</b>	<b>AD Authentication</b>	<b>10</b>			
5.1	Add/ Remove User from MS Active Directory	05			
5.2	Login using AD	05			
<b>6.0</b>	<b>Dashboard</b>	<b>10</b>			
6.1	Display pie chart of type of devices logged-in for a given duration. Devices includes Android, iOS	05			
6.2	Graph depicting number of Users logged into system for a given duration	05			
	<b>TOTAL</b>	<b>60</b>			

**Annexure-1 of Appendix-'J'**

**Technical QCBS - demo of Secure application container using Unified Endpoint Management (UEM) software**

*Note:*

(a) *Sample demo application of Bidders' existing Unified Endpoint Management (UEM) software application as POC. Bidder need to exhibit required software engineering expertise and UEM subject matter expertise to ICG Technical Evaluation Committee (TEC).*

(i) *Secure Application Container. Bidder to demonstrate sample of 100 Users environment with 10 endpoints including Android, iOS, Mac Book, Windows Laptop to bring out important Secure Application Container features to TEC.*

**POC Project Document** (Refer. Para-6(k) of Appendix-'G' of RFP). The Bidder should prepare document and submit Part-A as part of Technical Bid in following structure and provide detailed demo of Part-B during TEC

**Part-A: Project Document for POC** (20 Marks) [To be submitted with Technical Bid]

1.0: Title of POC demo project

2.0: Index

3.0: Executive Brief (Should be within single A4 size page)

4.0: User Requirement

4.1: Storyboard of sample secure chat episode to cover all POC modules

4.2: Use Cases for 4.1

4.2: Screenshots, description of each Use Case as per 4.2

**Part-B: POC Demonstration** (60 Marks) during POC to TEC

		<b>Marks</b>	<b>Scored</b>	<b>Qualified [Y/N] (&gt;= 50%)</b>	
<b>1.0:</b>	<b>Publish Applications</b>	<b>10</b>			Para-6(e) of Appendix-'G'
1.1:	Publish and push sample Android application to mobile	05			

		<b>Marks</b>	<b>Scored</b>	<b>Qualified [Y/N] (&gt;= 50%)</b>	
1.2	phone Update patch to Android app without end user intervention	05			
<b>2.0</b>	<b>Secure Chat integration</b>	<b>10</b>			
2.1	Publish and install Secure Chat application	05			
2.2	Send/ Receive One-to- One text message	05			
<b>3.0</b>	<b>Security</b>	<b>10</b>			
3.1	Open photo received from email within container using native email client	05			
3.2	Showcase received photo safely secured and not accessible from outside container	05			
<b>4.0</b>	<b>Native viewer</b>	<b>10</b>			
4.1	Secure Browsing	05			
4.2	Send/ receive email	05			
<b>5.0</b>	<b>AD Authentication</b>	<b>10</b>			
5.1	Add/ Remove User using MS Active Directory	05			
5.2	Login using SSO for two different applications from Android	05			
<b>6.0</b>	<b>Endpoint support</b>	<b>10</b>			
6.1	Install secure applications on Mac Book	05			
6.2	Install secure applications on Windows Laptop	05			
	<b>TOTAL</b>	<b>60</b>			

**Appendix-'K'**

**DETAILS OF PRIME BIDDER & CONSORTIUM OF VENDORS PROFILE**

1. Details of Prime Bidder and Consortium Vendors

Sl.	Vendor details (Indicate Prime Bidder)	Role in current project	Supporting Documents for project profile, experience, Certifications
(a)			
(b)			
(c)			

**Note:-**

(a) Prime vendor shall be responsible for entire project execution and project management. Prime Bidder must deliver atleast any of the 02 item/ services out of 03 item/ services of Secure Chat/ Secure Application Container/ IT infrastructure.

**Prime Bidder & Consortium Member Profile** (Fill-up provide separate sheet per vendor, in case of consortium)

Sl.	Profile	Details	Remarks
1.0	Company Name, Contact Person & Address		
1.1	Company turn-over with positive net worth	(a) 2015-16: Rs. _____ (b) 2016-17: Rs. _____ (c) 2017-18: Rs. _____	Positive net worth to be mentioned for past 03 years
1.2	Certifications	(a) CMMi-5: ___ Year (b) CMMi-3: ___ Year (c) ISO 27001: ___ Year (d) ISO 20000: ___ Year (e) ISO 9001: ___ Year	Any other certifications, if any. All certifications should be currently valid.
1.3	Branch Offices	(a) Total: ___ Nos. of branches in India & Employees: ___ Nos. (b) Total: ___ Nos. of branches in Abroad & Employees	

<b>Sl.</b>	<b>Profile</b>	<b>Details</b>	<b>Remarks</b>
1.4	Software project implemented in Central/ State/PSU organisations (Rs.25 Lakhs and more) in past 05 years	(a) Central Govt: ___ Nos. (b) State Govt: ___ Nos. (c) PSUs: ___ Nos. (d) Non-Govt/ Corp.: ___ Nos.	Indian/ Abroad projects be mentioned separately. Only relevant and key projects to be considered.
1.5	IT infrastructure & services project implemented in Central/ State/PSU organisations (Rs.25 Lakhs and more) in past 05 years	(a) Central Govt: ___ Nos. (b) State Govt: ___ Nos. (c) PSUs: ___ Nos. (d) Non-Govt/ Corp.: ___ Nos.	Indian/ Abroad projects be mentioned separately. Only relevant and key projects to be considered
2.0	Total manpower	(a) Software: ___ Nos. (b) ICT: ___ Nos. (c) India: ___ Nos. (d) Abroad: ___ Nos. (e) Total (b+c+d): ___ Nos.	India/ abroad manpower be separately mentioned. Parent company be excluded. Software/ ICT manpower separately mentioned.
2.1	Business Analyst	(a) CBAP certified: ___ Nos. (b) Non-Certified: ___ Nos.	
2.2	Sr. Software Architect	(a) Total: ___ Nos.	(a) Minimum experience as architect for 05 projects (b) Minimum of 05 year experience (c) Experience on CASE tools to architect software systems (d) Experience on ALM software such as JIRA (e) Experience on Project mgmt. software
2.3	Secure Chat Application Manpower	(a) Certified: ___ Nos. (b) Non-Certified: ___ Nos.	
2.4	Oracle Database	(a) OCP Certified, SQL/PLSQL: ___ Nos.	

<b>Sl.</b>	<b>Profile</b>	<b>Details</b>	<b>Remarks</b>
	Manpower	(b) OCP Certified, DBA: ____ Nos. (c) Non-Certified: ____ Nos.	
2.5	Project Management Manpower	(a) PMP Certified: ____ Nos. (b) MS Project/PrimaVera Certified excluding PMP: ____ Nos. (b) Non-Certified: ____ Nos.	
2.6	Oracle ADF Developers	(a) ADF Certified: __ Nos. (b) Non-Certified: __ Nos.	
2.7	Java Developers	(a) Java Certified: __ Nos. (b) Non-Certified: __ Nos.	
2.8	Testers	(a) Certified Testers: ____ Nos. (b) Non-Certified: ____ Nos.	
2.9	GUI Designers	(a) Certified Designers: ____ Nos. (b) Non-Certified: ____ Nos.	
3.0	Development/Support/DevOps Tools	(a) CASE Tools: _____ (b) Source Code Server: _____ (c) GUI Testing: _____ (d) Unit Testing: _____ (e) ALM Software: _____ (f) ITIL Service Desk: _____ (g) Project Mgmt: _____ (h) Java IDE: _____	(a) Computer Aided Software Engineering Tools such as Rational Software Architect etc. (b) Source Code Server such as Git/Subversion/ Bit bucket (c) GUI testing such as 'Selenium' etc. (d) Application Lifecycle Management (ALM) such as Atlassian JIRA, Confluence, Bamboo, Jenkins etc. (e) ITIL Service Desk as duly certified by PinkVerify© such as JIRA Service Desk, BMC etc. (f) 'Project Management' software such as MS Project, Oracle PrimaVera etc. (g) Java IDE such as Eclipse, IntelliJ IDEA, JDeveloper etc.
4.0	Demo application to	(a) Can you showcase a demo POC application during TEC to display your skillset on	POC demo application document need to be



<b>Sl.</b>	<b>Profile</b>	<b>Details</b>	<b>Remarks</b>
	exhibit skillset by vendor	<p>Analysis/Design/Development/ Test/Deployment and Maintenance? <u>[Yes/No]</u>.</p> <p>If Yes, following characteristics need to be included on POC application.</p> <p>(a) CASE tools usage for OOAD of project</p> <p>(b) MS Project/ Primavera for project planning/costing/duration</p> <p>(c) GUI design patterns for web application/ desktop applications</p> <p>(d) DevOps based development</p> <p>(e) Agile planning</p> <p>(f) Complete project from User Requirement to Testing on Agile to be based on any of ALM software such as JIRA and all related documents should be available on Confluence or equivalent</p> <p>(g) Testing for Black-box/ White-box and automated GUI testing</p> <p>(h) SOA/Micro services based architecture, deployed on Docker Containers</p>	submitted as part of Technical Bid and subsequently, during evaluation vendor need to provide live demo for given simple sample application.
6.0	Single point of Contact (SPOC-Business) for Coast Guard	<p>(a) Name: _____</p> <p>(b) Desig.: _____</p> <p>(c) Email: _____</p> <p>(d) Mobile: _____</p> <p>(e) Office location: _____</p>	
6.1	Single point of Contact (SPOC-Technical) for Coast Guard	<p>(a) Name: _____</p> <p>(b) Desig.: _____</p> <p>(c) Email: _____</p> <p>(d) Mobile: _____</p> <p>(e) Office location: _____</p>	
7.0	Any other information		Provide any other details as you may feel relevant to Coast

<b>Sl.</b>	<b>Profile</b>	<b>Details</b>	<b>Remarks</b>
			Guard.

Note: India/ abroad manpower to be mentioned separately.

**Instructions for Online Bid Submission:**

1. The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal.
2. More information useful for submitting online bids on the CPP Portal may be obtained at: <https://eprocure.gov.in/eprocure/app>.
3. **Registration**
  - (a) Bidders are required to enrol on the e-Procurement module of the Central Public Procurement Portal (URL: <https://eprocure.gov.in/eprocure/app>) by clicking on the link "**Online bidder Enrollment**" on the CPP Portal which is free of charge.
  - (b) As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.
  - (c) Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.
  - (d) Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / nCode / eMudhra etc.), with their profile.
  - (e) Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.
  - (f) Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / e-Token.
4. **Searching for tender documents**
  - (a) There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, Organization Name, Location, Date, Value, etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as Organization Name, Form of Contract, Location, Date, Other keywords etc. to search for a tender published on the CPP Portal.
  - (b) Once the bidders have selected the tenders they are interested in, they may download the required documents / tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the CPP Portal to intimate the bidders through SMS / e-mail in case there is any corrigendum issued to the tender document.
  - (c) The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification / help from the Helpdesk.

5. **Preparation of bids**

- (a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.
- (b) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents – including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.
- (c) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF/JPG formats. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.
- (d) To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Space" or "Other Important Documents" area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

6. **Submission of bids**

- (a) Bidder should log into the site well in advance for bid submission so that they can upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
- (b) The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document.
- (c) Bidder has to select the payment option as "offline" to pay the tender fee / EMD as applicable and enter details of the instrument.
- (d) Bidder should prepare the EMD as per the instructions specified in the tender document. The original should be posted/couriered/given in person to the concerned official, latest by the last date of bid submission or as specified in the tender documents. The details of the DD/any other accepted instrument, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time. Otherwise the uploaded bid will be rejected.
- (e) Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BoQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BoQ file, open it and complete the white coloured (unprotected) cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BoQ file is found to be modified by the bidder, the bid will be rejected.
- (f) The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the

bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

(g) All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data. The data entered cannot be viewed by unauthorized persons until the time of bid opening. The confidentiality of the bids is maintained using the secured Socket Layer 128 bit encryption technology. Data storage encryption of sensitive fields is done. Any bid document that is uploaded to the server is subjected to symmetric encryption using a system generated symmetric key. Further this key is subjected to asymmetric encryption using buyers/bid openers public keys. Overall, the uploaded tender documents become readable only after the tender opening by the authorized bid openers.

(h) The uploaded tender documents become readable only after the tender opening by the authorized bid openers.

(j) Upon the successful and timely submission of bids (ie after Clicking "Freeze Bid Submission" in the portal), the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.

(k) The bid summary has to be printed and kept as an acknowledgement of the submission of the bid. This acknowledgement may be used as an entry pass for any bid opening meetings.

## 7. **Assistance to bidders**

(a) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

(b) Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk.

**ABBREVIATIONS & TERMINOLOGY**

1. **Abbreviations**

<b>ABBREVIATION</b>	<b>ABBREVIATION DESCRIPTION</b>
<b>AD</b>	: Active Directory
<b>AHS</b>	: Allied Health Services
<b>AIAMC</b>	: All Inclusive Annual Maintenance Contract
<b>AMC</b>	: Annual Maintenance Contract
<b>ATS</b>	: Annual Technical Support
<b>Bidder</b>	: Vendor who participated in tender issued by ICG
<b>BPEL</b>	: Business Process Execution Language
<b>BPM</b>	: Business process management
<b>BPMN</b>	: Business Process Model and Notation
<b>Buyer</b>	: Indian Coast Guard
<b>CAL</b>	: Client Access License
<b>CDA(N)</b>	: Controller of Defence Account (Navy)
<b>CGHQ</b>	: Coast Guard Headquarters, New Delhi
<b>COTS</b>	: Commercially-Off-The-Shelf software
<b>CPC</b>	: Central Pay Commission
<b>CPMT</b>	: ICG Cloud Provisioning and Maintenance Team
<b>DISHA</b>	: Digital Infrastructure Services for Hosting Applications.
<b>EAD</b>	: Enterprise-class Agile Development
<b>EAI</b>	: Enterprise Application Integration
<b>EMM</b>	: Enterprise Mobility Management #
<b>EMS</b>	: Electronic Mail System
<b>GPON</b>	: Gigabit Passive Optical Network
<b>HA</b>	: High-Availability
<b>HQ.</b>	: Headquarter
<b>IC4</b>	: ICG Cyber Command and Control Center
<b>ICG</b>	: Indian Coast Guard

<b>ABBREVIATION</b>	<b>ABBREVIATION DESCRIPTION</b>
<b>IDC</b>	: ICG Interim Data Center
<b>IDR</b>	: ICG Disaster Recovery Data Center
<b>IPADS</b>	: Integrated Pay And Disbursement System (IPADS)
<b>IPD</b>	: In Patient Department
<b>ISP</b>	: Internet Service Provider, who provide internet services
<b>MAF</b>	: Manufacture Authorisation Form
<b>MAM</b>	: Mobile Application Management #
<b>MDM</b>	: Mobile Device Management #
<b>NAS</b>	: Network Access Storage
<b>NETRA</b>	: ICG Network of Tatrakshak Applications framework
<b>NGFW</b>	: Next Generation Firewall
<b>NOC</b>	: Network Operations Center
<b>OEM</b>	: Original Equipment Manufacturer
<b>OPD</b>	: Out Patient Department
<b>OU</b>	: Organisation Unit (OU) in ICG Active Directory
<b>PCDA(N)</b>	: Principle Controller of Defence Accounts (Navy)
<b>QCBS</b>	: Quality and Cost Base Selection
<b>RHQ</b>	: Coast Guard Regional Headquarters
<b>RWD</b>	: Responsive Web Design
<b>SaaS</b>	: Software as a Service
<b>SAN</b>	: Storage Area Network
<b>SDOT</b>	: ICG Software Development and Overseeing Team
<b>SI</b>	: System Integrator
<b>SIMHA</b>	: ICG Secured Integrated Management for Hosting Applications (SIMHA). ICG specific framework is based on Oracle Middleware stack.
<b>SOC</b>	: Security Operations Center
<b>SOW</b>	: Scope of Work
<b>TSP</b>	: Telecom Service Provider
<b>UEM</b>	: Unified Endpoint Management #
<b>WAF</b>	: Web Application Firewall

## 2. **General Terminology**

<b>TERMINOLOGY</b>	<b>TERMINOLOGY DESCRIPTION</b>
<b>AHS</b>	: Allied Health Services. It includes Laboratories, Pharmacies, Imaging, Therapies, Social and Psychological Support services etc, that provide both diagnostic and therapeutic support to both the OPD and IPD patients
<b>ATS</b>	: Annual Technical Support, provided by OEM for patches, upgrades, remote support etc.
<b>Bidder Buyer</b>	: Vendor who participated in tender issued by ICG : Indian Coast Guard
<b>CDA(CG)</b>	: Controller of Defence Account (Coast Guard)
<b>CGHQ</b>	: Coast Guard Headquarters, New Delhi
<b>COTS</b>	: Commercially-Off-The-Shelf software. To qualify as COTS software, product should have 10 years of maturity, atleast 03 certified support partners in India each having atleast 01 current client, product having atleast 10 current deployments, product to have dedicated support portal with datasheets/user manuals/ API manuals/admin manuals/ patches and published roadmap for next 05 years.
<b>CPMT</b>	: ICG Cloud Provisioning and Maintenance Team. It is responsible to provide all required IT infrastructure including compute/storage/network/security and IT middleware platform including SIMHA in support of most if the ICG software applications
<b>DISHA</b>	: Digital Infrastructure Services for Hosting Applications. A project of Coast Guard to deploy managed IT infrastructure.
<b>EMS</b>	: Electronic Mail System
<b>HA</b>	: High-Availability. A configuration to provide maximum availability of IT infrastructure & services.
<b>IC4</b>	: ICG Cyber Command and Control Center. It monitors and manages all aspects of ICG IT Operations including NOC, SOC, Cloud, Application Support and Service Desks. IC4 to operate 24x7x365.
<b>In-Rack/Row Cooling</b>	: An in-rack/row cooling system cools down the servers placed within closed in-rack/ in-row cabinets, providing microclimate within rack, having separate hot/ cold aisle containment at in-rack/ in-row level.
<b>IPD</b>	: In Patient Department. In includes areas of the hospital where patients are accommodated after being admitted, based on doctors/specialist's assessment, from the Emergency Services, Ambulatory Care, and Clinical/Specialty Outpatient Departments due to their presenting and emerging medical condition(s). Inpatients typically require a higher level of care and intensity of treatment, such as need for surgery, intensive medical, surgical or



<b>TERMINOLOGY</b>	<b>TERMINOLOGY DESCRIPTION</b>
	infection management, special observation and/or isolation, sustained therapy, or extensive testing.
<b>ISP</b>	: Internet Service Provider, who provide internet services
<b>NETRA</b>	: ICG Network of Tatrakshak Applications framework. Mother IT Framework provide end-to-end IT automation in ICG. It envisages five core domains including ERP for cradle-to-grave asset lifecycle of Acquisition/Maintenance/Logistics/Finance/HR, Non-ERP for office automation, IT infrastructure, Information Security and ICG Dashboard to provide high-level executive view.
<b>OPD</b>	: Out Patient Department. Caters to a population of patients who only need a consultation with a doctor/specialist and/or obtain ongoing medical treatment or services as a result of an earlier visit. Patients arrive, complete their appointment, and then leave the Outpatient Clinic or Department.
<b>OU</b>	: Organisation Unit (OU) in ICG Active Directory. Usually individual ICG units are to be considered as OU, which contain Users/Computers and managed as single unit. ICG SaaS enabled applications shall provide multi-tenancy at OU level which can be aggregated at various ICG admin authority levels. Typical OU within ICG context are ICG units such as ICGS Chennai, Admin Authority OUs are DHQ at State level, RHQ at Regional level, CGC at Western/Eastern Seaboard level and ICG level
<b>PCDA(N)</b>	: Principle Controller of Defence Accounts (Navy). Defence accounting office for Indian Navy & Indian Coast Guard located at Mumbai.
<b>QCBS</b>	: The method of selection is Quality and Cost Base Selection (QCBS). The weights given to the Technical and Commercial Bids are: Technical = 70% and Commercial = 30%
<b>SaaS</b>	: Software as a Service. ICG SaaS enabled applications should support multi-tenancy at OU level and shall be aggregated at various ICG admin authority levels. Typical OU within ICG context are ICG units such as ICGS Chennai, Admin Authority OUs are DHQ at State level, RHQ at Regional level, CGC at Western/Eastern Seaboard level and ICG level
<b>SDOT</b>	: ICG Software Development and Overseeing Team. Nodal institution under Directorate of IT, CGHQ responsible for overall software development to ensure compliance to ICG standards. SDOT shall act as Single-Point-of-Contact (SPOC) for all software projects.
<b>Seller</b>	: Vendor who participated in tender and issued supply/ work order by ICG
<b>SI</b>	: System Integrator. Bidder who is issued with work order to implement involving multifaceted implementations/provisioning of turn-key projects at ICG
<b>SIMHA</b>	: ICG unified middleware software platform standard framework Secured Integrated Management for Hosting Applications (SIMHA). It includes common Oracle middleware and database components of Enterprise Portal, API manager, BI Server, Enterprise Service Bus

<b>TERMINOLOGY</b>	<b>TERMINOLOGY DESCRIPTION</b>
	(ESB) Server, BPM, Case Management, DMS Server, RMS Server, J2EE Application Server and Oracle Database with Golden Gate replication, ADE, Label Security, Data Vault. All applications other than ERP should be built on SIMHA as per ICG NETRA Framework standards.
<b>SOC</b>	: Security Operations Center. Monitors & manages all information security aspects of ICG. It is implemented as part of IC4.
<b>TSP</b>	: Telecom Service Provider, who provide various telecom related services including MPLS, Leased Line & VSAT

### 3. Payroll Terminologies & Abbreviations

<b>ABBREVIATION</b>	<b>ABBREVIATION DESCRIPTION</b>
<b>Payroll</b>	: An Organisations' financial list of the salaries, wages, bonuses, net pay, and deductions of their employees
<b>Salary</b>	: Fixed amount per pay period
<b>Wage</b>	: Variable amount of pay usually by hour/day worked
<b>Retro pay</b>	: Compensation related to a previous pay period. You give retro pay later than when the initial pay took effect
<b>Back pay</b>	: Pay that is owed for past work or services rendered as the result of some sort of payroll or bookkeeping error or delay in processing
	:
	:
	:
	:
	:

*(Note: All abbreviations & terminology are within context of Coast Guard unless otherwise explicitly mentioned)*