Tele: 011-23019440
Fax: 011-21411710
E-Mail: awing-sys.mod@nic.in

File no. IT/3002/DCG/Dir(Systems)

Ministry of Defence
Systems Division, Acquisition wing
O/o Additional Director General
Acquisition Technical (Maritime& Systems)
Room No. 10, Ground Floor
New Delhi -110011

03 Nov 22

To,

REQUEST FOR TECHNICAL AND COMMERCIAL PROPOSAL FOR 'DIGITAL COAST GUARD (DCG)'PROJECT INCLUDING CORE IT INFRASTRUCTURE FOR ICG (DATA CENTRE, DISASTER RECOVERY DATA CENTRE, NEAR LINE DATA CENTRE, PAN ICG MPLS/ VSAT CONNECTIVITY) AND ERP PAKCAGE 'SAFAL' COMPRISING SURFACE & AVIATION OPS LOGISTIC, FINANCE AND HUMAN RESOURCE MANAGEMENT MODULES
CATEGORY: BUY INDIAN

Dear Sir/Madam,

1. The Ministry of Defence, Government of India, intends to implement the 'Digital Coast Guard (DCG)' project, which includes establishment of core IT infrastructure (Data Centre, Disaster Recovery Data Centre, Near Line Data Centre and a Pan ICG Network with connectivity extended to related CDA offices) & development of an ERP Package 'SAFAL' (Surface & Aviation ops Logistics, Finance and HR modules)) along with associated civil infrastructure, last mile connectivity, hardware, Technical Support. Also, Uptime Institute Tier-III Gold certification for design, build readiness, commissioning, construction monitoring, operation & maintenance for six years and seeks participation in the implementation process from prospective Bidders under the "Buy Indian category" subject to requirements in succeeding paragraphs.

Synopsis

2. **Broad Description of Equipment/System**. The Digital Coast Guard project to be implemented on turnkey basis. The project includes establishment of core IT infrastructure for Indian Coast Guard and development and implementation of ERP Package for digitisation and automation of Surface & Aviation ops Logistics, Finance and HR management processes in Indian Coast Guard. Details are as follows:-

(a) **Core IT Infrastructure**. The proposal for Digital Coast Guard (Core IT Infrastructure) would comprise following :-

(i) Construction of Uptime institute Tier-III certified one Data Centre at Noida/NCR, one Near Line Data Centre (NLDC) at Noida/NCR and one Disaster Recovery Data Centre at New Mangalore.

(ii) Air gapped intranet, internet zones and Security Operation Centre (SoC) along with allied facilities.

(iii) Establishment of pan ICG MPLS/ VSAT Wide Area Network providing connectivity to 109 nodes (210 links) of ICG and PCDAs/ CDAs. Each site is to be connected with two redundant lines sourced from two different service providers. One-year bandwidth charges to be paid by System Integrator.

(b) **ERP Package 'SAFAL'**. The SAFAL ERP package intends to achieve automation and digitisation of Surface & Aviation ops Logistics, Finance and Human Resource Management processes for various day to day administrative operations of ICG. The software will be hosted in the ICG Data Centre (DC) and Disaster Recovery Data Centre (DRDC) and access will be provided to various users through ICGWAN.

(c) The DCG project will be under 02 yrs warranty followed by 03 yrs AIAMC.

(d) Onsite manpower support for 05 yrs.

3. The salient aspects and timelines of the acquisition are tabulated below. In case of any variation in the details furnished below or in any Annexures(s) with that mentioned in the RFP, information furnished in the main body of the RFP at referred Paragraph is to be followed: -

Sl.	Description	Details	Reference Para of the RFP
(a)	Equipment/System required	(i) Establish core IT infrastructure for the Indian Coast Guard along with allied facilities. (ii) Enterprise Resource Planning (ERP) package 'SAFAL' for automation and digitization of all aspects related to Surface & Aviation ops Logistics, Finance and HR management processes in ICG. (iii) 02 yrs warranty followed by 03 yrs AIAMC. (iv) Manpower support for 05 yrs.	Para 2, Page 1
(b)	Quantity Required	One Data Centre (DC), one	Para 2, Page 1

Sl.	Description	Details	Reference Para of the RFP
		Disaster Recovery Data Centre (DRDC), one Near Line Data Centre (NLDC) at CG land and a pan ICG MPLS/ VSAT WAN (109 sites/ 210 links) and one ERP package comprising of Surface & Aviation ops Logistics, Finance and HR modules including two years warranty followed by three years AIAMC and onsite manpower support for five years.	
(c)	Categorisation of Procurement	Buy Indian	Para 1, Page 1
(d)	Minimum IC Content required	45%	Para 7, Page 11
(e)	Place(s) of Delivery	Designated ICG consignees	para 1.1.1., Appendix 'H', Page 446
(f)	Warranty Period	Two years	Para 12, Page 12
(g)	AIAMC Period, if any	Three years on expiry of Two years Warranty period	Para 14(a), Page 13
(h)	Offsets required, if any	No	-
(j)	EMD Amount	₹2 Crores	Para 8.2 of Annexure to Appendix 'K', Page 482
(k)	Last date for submission of Pre-bid queries	As indicated in RFP	Para 22, Page 15
(l)	Date and time for Pre-bid meeting	As indicated in RFP	Para 23, Page 15
(m)	Last date and time for Bid Submission	As indicated in RFP	Para 24, Page 15

4. **Special features of the *RFP*.**

(a) The core IT infrastructure being envisaged under this RFP is required to integrate and subsume the existing IT infrastructure in ICG. The functional requirements and implementation of the private cloud for ICG will be fully integrated with the supplied and existing hardware/ software i.e., integration with manager of the hypervisor, Software Defined Network and storage, etc. The CMP (Cloud Management Platform) will be integrated with the existing Directory Service software and will create business group as per the requirements given by ICG. Details of the integration requirements are placed at **Annexure I to Appendix A** to this RFP.

(b) Proposed ERP application should be able to interface with existing ICG applications deployed on ICG Middleware Platform (SIMHA) such as ASHA, PARAM, BRASS etc. for bi-directional data transfer without any licensing restrictions. Details of existing applications required to be integrated at ICG middleware 'SIMHA' are placed at **Annexure II** to ***Appendix A***. Preferably, the application should expose key functions as web services for third party interfacing and integration. The details may be given in technical bid for interface possibilities. Also PARAM forms/Gx, YATRA ICG portal can also be migrated to proposed ERP solutions. An integrated portal to view selected information should be developed on middleware platform 'SIMHA' as part of 'Unified ICG Portal' architecture requirements. Supply of Enterprise Database licenses as required including offline remote replication support for ICG Ships and internet zone. The proposal to include warranty for two years (including ATS) followed by AIAMC support for three years (including ATS) post final acceptance and go-live of ERP.

(c) **User Acceptance Trials**. For an equipment to be introduced in service, it is mandatory that it successfully clears all stipulated tests/ trials/ evaluations as per RFP. The equipment in subject project shall be subjected to on site acceptance trials before go-live.

(d) **Go-Live/ Project Completion**. Project will be considered as completed on fulfilment of below mentioned conditions: -

(i) Establishment of Civil infrastructure for Data Centre, Diaster Recovery Data Centre & Near Line Data Centre as per specifications mentioned at Appendix A and acceptance by ICG.

(ii) Completion of Desgin & Construction Certification from Uptime Institute.

(iii) Completion of LEEDS certification for Green Building Norms.

(iv) Completion of Delevery, Installations and Commissioning of all IT hardware (DC, DRDC, NLDR, ROBO racks for ships and ERP production hardware) as per the specifications given at Appendix A and as per the approved bill of material.

(v) Submission of all design specifications drawings, architectural drawings of civil infrastructure, OEM equipment manuals (Operations, Maintenance & Training) and Warranty & Guarantee Certificates.

(vi) Final acceptance by ICG Team for DC, DRDC, NLDC operability, synchronisation and automation with maximum load capacity.

(vii) Acceptance of all deliverables of ERP as per the SRS and after completion of security audit by Cert-In empanelled vendor. Proving of Offline capability.

(viii) Submit all licenses and codes in respect of ERP SAFAL and solutions deployed in DC, DRDC & NLDC.

(ix) Provisioning and proving of NMS with establishment of redundant network at 109 sites.

(x) Positioning of Manpower as per the requirement projected at para 255 of Appendix 'A'.

(xi) Establishment of NOC and SOC with single integrated display.

(xii) Signing of workdone certificate by the ICG.

(e) Although completion of various sub-activities on civil work, delivery, installation and commissioning of hardware of DC, DRDC and NLDC, establishment of network and development of ERP solution entitle the bidder for corresponding stage payments, the project is deemed to be completed only on completion of activities mentioned at para 4(d) above in its entirety to get eligible for payment against **Sl. (j)** of **Annexure-V** to **Appendix-H** of this RFP.

(f) Selection of the vendor will be on two bid system. Commerical offer of qualified vendors in TEC will be considered for deciding L1.

5. This Request for Proposal (RFP) consists of following four parts:-

Ser No.	Description	Page
(a)	Part I - General Requirements	10-16
(b)	Part II - Technical Requirements	17-28
(c)	Part III - Commercial Requirements	29-30
(d)	Part IV - Bid Evaluation and Acceptance Criteria	31

6. The Government of India invites responses to this request only from reputed firms, developers and system integrators duly authorized by their OEM partners (Licenses/ software and hardware).

7. The end user of the equipment is the Indian Coast Guard.

VERIFIED

8. This RFP is being issued with no financial commitment and the Ministry of Defence reserves the right to withdraw the RFP and change or vary any part thereof or foreclose the procurement case at any stage. The Government of India also reserves the right to disqualify any Bidder should it be so necessary at any stage on grounds of National Security.

9. This RFP is non-transferable.

10. In addition to various Appendices and their Annexures, attached with this RFP, reference to various paragraphs of DAP-2020 has been made in the RFP. The DAP - 2020 is an open domain document that is available at GoI, MoD website www.mod.nic.in.

11. The receipt of the RFP may please be acknowledged.

Yours faithfully,

(Pushpender Choudhary)
Col
Director (Systems)
O/o ADG Acq Tech (Maritime & Systems)
Acquisition Wing/ Ministry of Defence

Distribution:-

1. Copy No. 1 : O/o ADG Acquisition Technical (M&S)
2. Copy No. 2 : Steering Direcortate of SHQ
3. Copy No. 3 : Plannning Directorate of SHQ
4. Copy No. 4 : FM (M&S)/ IFA (Capital)
5. Copy No. 5 : Web hosting on the websites as given below
    (i) www.mod.in
    (ii) www.tenders.gov.in
    (ii) www.indiancoastguard.gov.in

VERIFIED

INDEX

VERIFIED

Annexure/ Appendix	**Description**	**Reference**
Appendix-O	Document to be submitted by the bidder along their Techno- Commercial proposal	Part IV
Appendix P	Software Artefacts and Associated IPR	Part I
Appendix Q	Bill of Material	Part III
Appendix R	Project Management	Part II

Disclaimer

1. This RFP is neither an agreement and nor an offer by the MoD to the prospective Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in submitting their proposals pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by the MoD in relation to the Project. This RFP document and any assumptions, assessments and statements made herein do not purport to contain all the information that each Bidder may require. The Bidder shall bear all its costs associated with or relating to the preparation and submission of proposal pursuant to this RFP. Wherever necessary, MoD reserves the right to amend or supplement the information, assessment or assumptions contained in this RFP. The MoD reserves the right to withdraw the RFP or foreclose the procurement case at any stage. The issuance of this RFP does not imply that the MoD is bound to shortlist a Bidder for the Project. The MoD also reserves the right to disqualify any Bidder should it be so necessary at any stage on grounds of National Security.

PART I - GENERAL REQUIREMENTS

1. This part consists of the general requirement of the Goods (also referred as equipment/ systems/deliverables) and Services, hereafter collectively referred as 'Deliverables', the numbers required, the time frame for deliveries, conditions of usage and maintenance, requirement for training, Life cycle support management, AIAMC and warranty/ guarantee conditions, etc. It includes the procedure and the date & time for submission of bids.

Non-Disclosure

2. The Bidding documents, including this RFP and all attached documents provided by the MoD, are and shall remain or become the property of the MoD. These are transmitted to the Bidders solely for the purpose of preparation and the submission of a proposal in accordance herewith. Bidders are to treat all information as strictly confidential and shall not use it for any purpose other than for preparation and submission of their proposal. The provisions of this Para shall also apply mutatis mutandis to Bids and all other documents submitted by the Bidders and the MoD will not return to the Bidders any proposal, document or any information provided along therewith (except unopened Commercial Bid and EMD, as relevant).

3. Information relating to the examination, clarification, evaluation and recommendation for the Bidders shall not be disclosed to any person who is not officially concerned with the process, or concerning the Bidding Process. The MoD will treat all information, submitted as part of the Bid, in confidence and will require all those who have access to such material to treat the same in confidence. MoD may not divulge any such information unless it is directed to do so by any statutory entity that has the power under law to require its disclosure or is to enforce or assert any right or privilege of the statutory entity and/ or MoD or as may be required by law or in connection with any legal process.

4. **Confidentiality of Information**. No party shall disclose any information to any 'Third Party' concerning the matters under this RFP generally. In particular, any information identified as 'Proprietary' in nature by the disclosing party shall be kept strictly confidential by the receiving party and shall not be disclosed to any third party without the prior written consent of the original disclosing party. This clause shall apply to the sub-contractors, consultants, advisors or the employees engaged by a party with equal force. The bidder and buyer have to sign a non-disclosure agreement as per format placed at **Appendix M** to RFP.

5. **Business Eligibility**

5.1 **Undertaking by Bidders**. The Bidder will submit an undertaking that they are currently not banned / debarred / suspended from doing business dealings with Government of India / any other government organisation and that there is no investigation going on by MoD against them. In case of ever having been banned / debarred / suspended from doing business dealings with

MoD/any other government organization, in the past, the Bidder will furnish details of such ban / debarment along with copy of government letter under which this ban/ debarment / suspension was lifted/ revoked. The Bidder shall also declare that their sub-contractor(s)/ supplier(s)/ technology partner(s) are not Suspended or Debarred by Ministry of Defence. In case the sub-contractor(s)/ supplier(s)/ technology partner(s) of the Bidder are Suspended or Debarred by Ministry of Defence, the Bidder shall indicate the same with justification for participation of such sub-contractor(s)/ supplier(s)/ technology partner(s) in the procurement case.

5.2 Subsequent to submission of bids if any sub-contractor(s)/ supplier(s)/ technology partner(s) of the Bidder is Suspended or Debarred by Ministry of Defence, the Bidder shall intimate the Ministry of Defence regarding Suspension or Debarment of its sub-contractor(s)/ supplier(s)/ technology partner(s) within two weeks of such order being made public.

6. **Pre-Qualification Criteria**. The detailed Prequalification criteria for the Bidders for participation in the instant procurement case are placed at **Appendix N** to this RFP. All Bidders are to submit details as per the criteria along with the Technical Bids. These would be evaluated by the TEC.

7. **Indigenous Content**. For the purposes of this RFP and the acquisition contract (if any) signed by the Ministry of Defence with a successful Bidder, indigenous content shall be **minimum 45%** as defined under **Para 1** of **Appendix B** to **Chapter I** of **DAP-2020**. In addition, reporting requirements for prime (main) Bidders (and for sub-contractors/ suppliers/ technology partners reporting to higher stages/ tiers) shall be as prescribed under **Para 4 to 7** of **Appendix B** to **Chapter I** of **DAP-2020** ***(or as approved by AoN according authority)***. The right to audit Bidder/ sub-contractors/ suppliers/ technology partners shall vest in the Ministry of Defence as prescribed under **Para 10**; and aspects of delivery, certification, payments, withholding of payments and imposition of penalties shall be as prescribed under **Para 11** to **15** thereof. Furthermore, Bidders will be required to submit their indigenisation plan in respect of indigenous content as stipulated in **Para 4 to 7** of **Appendix B** to **Chapter I** and **Para 39** of Chapter II of DAP 2020. The DAP 2020 is available at MoD, GoI website (www.mod.nic.in) for reference and free download.

8. **Year of Production**. Deliverables [platforms (including major equipment)/ equipment/ systems] supplied under the contract should be of latest manufacture i.e manufactured after the date of Contract with unused components/ assemblies/ sub-assemblies conforming to the current production standard and should have 100% of the defined life (other than permitted running hours during assembly/ acceptance trials) at the time of delivery. Deviations if any, should be clearly brought out by the Bidder in the Technical Proposal.

9. **Delivery Schedule**. The entire project is required to be delivered within 24 months from the date of signing of the contract. The delivery schedule of equipment

and services along with the relevant payment stages is specified at ***Annexure* V to *Appendix* 'H'**.

10. Once the contract is concluded and the delivery schedule is established, the Bidder shall adhere to it and ensure continuity of supply of deliverables and their components under the contract.

11. **Preservation *(as applicable)***. The hardware supplied as part of the core IT infrastructure & ERP Package are to be kept in safe custody post-delivery/ JRI/ *(to be as per delivery schedule at Para 9* until their installation and commissioning. In case, JRI necessitates unpacking to the extent that the preserved life of the deliverables is affected, Bidder is to undertake re-packing to restore the preserved life until the final installation/ commissioning at his own cost. In cases of any delay in STW/installation/integration trials/commissioning, attributable to the Buyer, the deliverables are to be re-preserved by the Bidder against payment of de-preservation/ re-preservation charges as per price quoted in the Price Bid. To facilitate this, the cost of in-storage/ in-situ de-preservation/ re-preservation, as applicable, is to be indicated in the Price Bid. This cost quoted by the Bidders at Sl (l) of Price bid format at ***Appendix 'J'*** would be counted towards determination of L1 and will be paid as per the price quoted if the service is utilized for extending the preserved life. In the cases where installation and trials is part of the Contract, the warranty will commence from the date of successful completion of go-live. In cases where the delay for installation, trials and commissioning is not attributable to the Bidder, payment terms for the stage related to installation and commissioning will be in accordance with ***Annexure V*** to ***Appendix* H.**

12. The deliverables supplied shall carry a warranty for **24** months. Commencement of warranty will be from the date of acceptance/ go-live, whichever is later. Warranty Clause is given at **Appendix C** to this RFP. The warranty of 24 months will comprise the Civil Infrastructure, Core IT infrastructure (functional Data Centre, functional Disaster recovery Data Centre, functional Near Line Data Centre, operational network and hardware installed on-board ships) and ERP Applications including all associated hardware/ software (including licenses and associated Annual Technical Support), goods/ stores supplied under the contract and each component used in the manufacture thereof shall be free from all types of defects/ failures post final acceptance of the DCG project or go live, whichever is later. The Seller also warrants that the civil infrastructure supplied/ delivered as part of the project would also remain free of any structural/ manufacturing defects during the period of warranty.

13. **In Service Life/ Shelf Life**. In Service of the deliverables should be minimum 7 years for IT HW and software, 15 years for DG sets, UPS & associated

equipment & 20 years for Civil Infrastructure. The Bidder is required to give details of reliability model, reliability prediction and its validation by designer/ manufacturer to ensure reliability of stores throughout Service/ shelf life. The efficacy of reliability model/ prediction/ validation would be verified during technical evaluation as indicated in Para **37** of this RFP.

14(a). **Product Support**. The Bidder would be bound by a condition in the contract that he is in a position to provide product support in terms of maintenance, materials and spares for a minimum period of five (05) years (two years warranty followed by three years AIAMC) post acceptance of the complete project i.e. functional Data Centre, functional Disaster recovery Data Centre, functional Near Line Data Centre, an Operational Network and functional ERP Application. Also, Bidder to provide product support for the software, licences, stores, assemblies/ sub-assemblies, fitment items and consumables, Special Maintenance Tools (SMT)/ Special Test Equipment (STE) subcontracted from other agencies/ manufacturers including warranty as per RFP after the delivery of project. Even after the said mandatory period, the Bidder would be bound to give at least two years notice to the Government of India prior to closing the production line so as to enable a Lifetime Buy of all spares before closure of the said production line. This, however, shall not restrict the Buyer from directly sourcing sub- equipment/ subassembly and spares from their respective OEMs/ sub-vendors on completion of warranty. In case the sub-equipment/ sub-assembly/ parts require tuning/ calibration/ integration by the Bidder prior replacement, the same is to be undertaken by the Bidder at fair and reasonable cost, as mutually agreed between Buyer and Bidder.

14(b). **Codification**. The Bidder agrees to provide existing NATO Stock Numbers (NSNs) of OEM for each item supplied under the contract as per part list (including MRLS). In case, the NSNs are not available, the bidder agrees to codify using basic technical characteristics as required for codification in consultation with MoD/ Directorate of Standardisation. In case of IPR issues, codification will be undertaken as Type IV codification (where only the manufacturer details and part number are to be provided).

15. **Obsolescence Management Plan**. An actionable obsolescence management plan is to be proposed by the Bidder along with the mechanism for intimation of notification of obsolescence. The modalities of the mechanism for intimation of notification would be deliberated during CNC. The mutually agreed mechanism for intimation would form an integral part of the contract. All upgrades and modifications carried out on the equipment during its life cycle i.e. 7 years for IT HW and software, 15 years for DG sets, UPS & associated equipment must be intimated to the SHQ as per the agreed mechanism.

16. **Training of Crew and Maintenance Personnel**. Training for all identified staff to be conducted for various roles of administration, support (L1/L2) of Main Data Centre, DR Data Centre, Networking and SAFAL ERP users to enable them to effectively operate and perform the relevant services using the software. The training content will have to be relevant to the target trainees depending upon the role. This training shall be designed to give the operators and maintainers (L1 & L2) necessary knowledge and skills to operate & Maintain-Data Centre, Disaster Recovery Data Centre, SAFAL ERP Package and associated hardware. The syllabus of the training should be defined by the Bidder in consultation with the Buyer at least six months prior offering the system for acceptance/ expiry of the delivery timeline. All training requirements such as training aids, projection system, complete equipment with accessories/ optional, technical literature as per ***Annexure-II*** *of* ***Appendix F***, spares, test equipment/ test set up, charts, training handouts, power point presentations, Computer Based Training (CBT), Documentation, Simulators etc will be catered by the Bidder. Training is to be provided as per **Annexure III** to **Appendix F** of this RFP.

17. **Government Regulations**. It may be confirmed that there are no Government restrictions or limitations in the countries from which sub-components are being procured and/ or for the export of any part of the deliverables being supplied.

18. It may be further confirmed that all national and international obligations relevant to countries from which parts and components are being procured, have been taken into account for the duration of the contract. Accordingly, thereafter there would be no review, revocation or suppression of Defence export license and other related clearance issues to the supplier for the contract that could impinge on the continuity of supply of items and their parts or components under the contract.

19. **Patent Rights.** The Bidder should confirm that there are no infringements of any Patent Rights in accordance with the laws prevailing in countries of the OEMs from whom equipment/ systems have been sourced. List of potential software artefacts and associated IPR is placed at **Appendix 'P'**.

20. **Integrity Pact**. In the subject RFP, The Bidders are required to sign and submit Pre Contract Integrity Pact (PCIP), given at ***Annexure to Appendix K*** to this RFP.

21. **Fall Clause**. If the equipment being offered by the Bidder has been supplied/ contracted with any organisation, public/ private in India, the details of the same may be furnished in the technical as well as commercial offers. The Bidders are required to give a written undertaking that they are not supplying the similar systems or subsystems at a price lower than that offered in the present bid to any other Ministry/

Department of the Government of India and if the similar system has been supplied at a lower price, then the details regarding the cost, time of supply and quantities be included as part of the commercial offer. In case of non-disclosure, if it is found at any stage that the similar system or subsystem was supplied by the Bidder to any other Ministry/ Department of the Government of India at a lower price, then that very price, will be applicable to the present case and with due allowance for elapsed time, the difference in the cost would be refunded to the Buyer, if the contract has already been concluded.

Bid Timelines

22. Any queries/ clarifications to this RFP may be sent to this office by 23 Nov 22 (date). A copy of the same may also be sent to:-

The Director General
[Project Director (Indigenisation & DCG project)]
Room No. 49
Coast Guard Headquarters,
National Stadium Complex, Purana Quila Road
New Delhi 100001
Email: dte-indg-dcg@indiancoastguard.nic.in

23. **Pre-Bid Meeting**. A pre-bid meeting will be organised by CGHQ at 1100 hrs on 14 Dec 22(date) at CGHQ (venue) to answer any queries or clarify doubts regarding submission of proposals. The Bidder or his authorised representative is requested to attend. Necessary details may be sent a week in advance to Project Directorate (Indg & DCG Project), Coast Guard Headquarters, to facilitate obtaining of security clearance. Pre-bid queries will be accepted from the prospective System Integrators (SIs) only.

24. **Submission of Bids**. The Technical and Commercial Proposals along with IP and EMD should be sealed separately in three separate envelopes clearly indicating Commercial/ Technical/ IP and EMD and any other Bank guarantee, as applicable, and then put in one envelope and sealed **(all the envelopes should clearly state the letter No of RFP and Name of the Project, Bidder name & Bid validity)** and submitted to the undersigned at the following address by 1200 hours on 24 Janb 23:-

Ministry of Defence
Systems Division, Acquisition Wing
O/o Additional Director General Acquisition Technical (Maritime & Systems)
Room No. 10 Ground Floor,
D-11 Wing, Sena Bhawan
New Delhi – 110 011

Tele: 011-23019440
Fax: 011-21411710
Email: awing-sys.mod@nic.in

25. Offer opening by Offer Opening Committee will be held at 1400 hrs on 24 Jan 23 at the same venue as indicated at Para 24 above. The Bidder or his authorised representative is welcome to be present at the opening of the proposals. Necessary details may be sent atleast one week in advance to facilitate obtaining of security clearance.

PART II - TECHNICAL REQUIREMENTS

26. The second part of the RFP incorporates the aspects of SQRs describing the technical parameters of the proposed equipment, and the environmental parameters for functioning. The operational characteristics and features that should be met by the equipment are elucidated at ***Appendix A*** to this RFP and the Compliance Table at ***Appendix B*** to this RFP. The Bidder would be required to submit the documents in support of the pre-qualification, compliance to technical requirement during TEC stage. The offered ERP solution will be subjected to a detailed User Acceptance Trials (UAT) post developmental phase during acceptance prior to go-live.

27. **Operational Characteristics and Features.** The broad operational characteristics and features that are to be met by the IT Infrastructure and SAFAL ERP envisaged under the DCG project are elucidated at ***Appendix A*** to this RFP.

28. **Technical Offer**. The Technical Offer must enable detailed understanding of the functioning and characteristics of the IT Infrastructure and SAFAL ERP envisaged under the DCG project as a whole and each sub system/ module independently. It must include the performance parameters as listed at ***Appendix A*** to this RFP and any other information pertaining to the technical specifications of the equipment considered important/ relevant by the Bidder. The technical proposal should also include maintenance schedules/ proposed modalities to be followed during the period of warranty and AIAMC to achieve maximum life and expected life of each module including licenses, associated hardware, assembly/ subassembly storage conditions/ environment condition recommended and the resultant guaranteed in-service/ shelf life.These would be evaluated TEC.

29. If there is any associated optional equipment and or module/ licenses on offer that should also be indicated separately along with the benefit that are likely to accrue by procuring such optional equipment. Should the Bidder be contemplating any upgrades or modifications to the equipment being offered as part of the IT Infrastructure and SAFAL ERP, the details regarding these should also be included in the Technical Proposal.

30. **Technical Details**

30.1 The technical details should be factual, comprehensive and include specifications of the offered system/ equipment being used as part of the IT Infrastructure, ERP package, enterprise emailing system and Central Portal as a whole and each module independently against broad requirements listed in ***Appendix A*** to this RFP. Project Digital Coast Guard broadly cover following: -

30.1.1 Construction of Uptime certified Tier – III Gold standard Data Centre, Disaster Recovery Data Centre, near Line Data Centre at Coast Guard provided clear land.

30.1.2 Air gapped intranet, internet zones and Security Operation Centre (SOC) infrastructure along with allied facilities, technical manpower and life cycle maintenance support (two years warranty followed by three years AIAMC).

30.1.3 Establish a pan ICG MPLS/ VSAT Wide Area Network providing connectivity to 109 nodes (210 links) of ICG (including jetties) and PCDAs/ CDAs and associated links activation & ground hub/ stations, as required. Each site is to be connected with two redundant lines sourced from two different service providers. The System Integrator has to pay the bandwidth charges pertaining to the links for one year.

30.1.4 The SAFAL ERP package for automation and digitisation of Surface & Aviation Ops Logistics, Finance and Human Resource management process modules for various day to day operations of ICG. The software will be hosted in the ICG Data Centre (DC) and Disaster Recovery Data Centre (DRDC) and access will be provided to various users through ICGWAN.

30.2 Insufficient or incomplete details may lead to rejection of the offer. Mere indication of compliance may be construed as incomplete information unless system's specific technical details are available in the offer. A format of the compliance table for the technical parameters and other conditions of RFP is attached as ***Appendix B*** to this RFP.

31. The technical offer should have a separate detachable compliance table as per format given at ***Appendix B*** to this RFP stating specific answers to all the parameters as listed at ***Appendix A*** to this RFP. It is mandatory to append answers to all the parameters listed in ***Appendix A*** to this RFP. Four copies of the Technical Proposal should be submitted (along with one soft copy), however only one copy of the commercial proposal is required (Copy of commercial offer should be annonated with name of project, bidder details & validity period/ date of quote).

32. **Submission of Project Report**

32.1 **Preliminary Project Report (PPR)**. A PPR must be submitted along with the Technical Offer. The PPR should indicate the methodology proposed to be adopted by the Bidder to execute the program and meet the delivery schedule laid down in the RFP. The PPR has to be submitted in the format placed at ***Appendix D.*** The PPR should broadly cover the following aspects:-

32.1.1 Project overview.

32.1.2 Definitions of key milestones based on indicative list of milestones and broad range of timelines specified at Para 45 of this part.

32.1.3 Broad plan for execution of the Project as per delivery schedule indicated at Para 9 of Part I of this RFP.

32.1.4 Lifetime product support plan.

32.1.5 Plan for meeting the Indigenous Content (IC) stipulated in the RFP.

32.1.6 Project organization structure as applicable.

32.2 **Project Report (PR)**. Post contract, the L1 Bidder will submit a PR covering the key aspects highlighted in the PPR and detailed project implementation plan.

33. **Malicious Code Certificate**. The Bidder and OEM is required to submit a **'Malicious Code Certificate'** along with the Technical Proposal. The format is placed at ***Appendix* E** to this RFP. In order to ensure mitigation of cyber/ information security threats, details of all the active components in the equipment being supplied along with their origin (i.e., OEM and country/ place of manufacture) are to be provided by the Bidders. Details of information security and cyber security requirements required to be complied by the bidder is placed at ***Annexure-III*** to ***Appendix 'A'*** to this RFP. Bidders need to provide the details of High Active and Active component in prescribed format placed at ***Annexure-III*** to ***Appendix 'A'***. Bidders have to undertake mandatory Security Audit & VA (Vulnerability Analysis) of Hardware, ERP Application etc. by CERT-IN empanelled firms.

34. **Product Support (Warranty/AIAMC)** After acceptance/ go-live, whichever is later, the technical support for the DC/ NLDC/ DRDC Hardware and ERP solution would be extended as per the warranty clause **(Appendix 'C')** and repair and maintenance philosophy at ***Appendix F*** to this RFP. The details of AIAMC, must also be submitted separately by the Bidder with technical aspects being included in the technical offer and commercial aspects being included in the commercial offer.

35. **Active Technology Obsolescence Management**. Bidder is to indicate the methodology on how the Bidder intends to undertake Active Obsolescence Management through life cycle of equipment 7 years for IT HW and software, 15 years for DG sets, UPS & associated equipment which would include upgradation of system/ sub-system/ units on completion of its fair service life. The Bidder/ OEM (as applicable) shall also intimate Buyer on likely technology obsolescence of various sub- assemblies/ units/ modules of equipment through an Annual Bulletin. In case of impending obsolescence of components, bulletin should specify either alternate item or option for lifetime buy as under:-

> 35.1 The Bidder/ OEM as applicable will notify the Buyer not less than two years before the closure of its production line about the intention to close production of equipment for provision of purchasing spare parts, before closure of the said production line.
>
> 35.2 Three years prior to completion of design/ service life of equipment, the Bidder/OEM (as applicable) will submit techno-commercial proposal for upgradation of equipment, wherever applicable, to mitigate technology obsolescence and for ensuring product support for next 7 years for IT HW and software, 15 years for DG sets, UPS & associated equipment if sought by ICG.

Evaluation of Technical Offers

36. The Technical Offer submitted by the Bidder will be evaluated by a Technical Evaluation Committee (TEC) to confirm that the equipment being offered meets the Essential Parameters as elaborated at ***Appendix A.*** The technical proposals will be evaluated on the mandatory Pre-qualification criteria and technical compliance as per RFP by TEC committee.

37. For an equipment to be introduced in service, it is mandatory that it successfully clears all stipulated tests/ trials/ evaluations as per RFP. The trial evaluation process is placed at **Appendix 'G'**.

38. Commercial bids of only those bidders who qualify in the Pre-qualification criteria would be opened.

Quality Assurance Instructions & Technical Evaluation Plan

39. For JRI of the supplied equipment, evaluation of the MVP and MVCR in respect of the individual modules of the ERP package and Final User Acceptance Trials of the entire project including, functional DC, DRDC, WAN and the ERP solution, Bidder would be required to submit a draft Acceptance Test Procedure (ATP) at least one month

before scheduled evaluation/ trials. The draft ATP submitted by the Bidder must include Quality Assurance Plans (QAP) as per OEM latest standards in vogue i.e. tests undertaken to assure quality and reliability and provide the Standard Acceptance Test Procedure (ATP). Based on the draft ATP, the ATP will be finalised by the Buyer. The Quality Assurance (QA) agency/ Board of Officers appointed by the Indian Coast Guard/ IPMG reserves the right to modify the ATP if necessary. ATP will also lay down the tests to be carried out during PDI and JRI. It shall be ensured that there are no repetition of QA tests in PDI and JRI. The JRI would normally be restricted to quantitative checks only, except where check proof is required to be carried out. In case PDI/ JRI are planned to be conducted by authorised Third Party Inspection (TPI) Agencies/ Buyers nominated QA agency, the same will be spelt out and the details included in the finalised ATP. QA of equipment will be carried out as per finalised ATP. For technical trials by QA agencies, the Bidder will arrange for requisite test facilities at OEM premises/ accredited laboratories for establishing conformance. The successful Bidder would also be required to provide those test facilities at OEM premises/ accredited laboratories/ mutally agreed place for quality assurance, which are not available with QA agencies. Details of the same will be included in the finalized ATP. Details of evaluation criteria are placed at **Appendix 'J'.**

Marking and Packaging

40. **Marking of Deliverables**. The Bidder shall ensure that each deliverable is marked clearly and indelibly, as follows:-

40.1 In accordance with the requirements specified in the RFP or if no such requirement is specified, with the indicated codification number or alternative reference number specified.

40.2 Ensure that any marking method used does not have a detrimental effect on the strength, serviceability or corrosion resistance of the deliverables.

40.3 Where the deliverables have a limited shelf life, with the cure date/ date of manufacture or expiry date expressed as months and years.

41. Where it is not possible to mark a deliverable with the required particulars, these should be included on the package in which the deliverable is packed.

42. **Packaging of Deliverables**. The Bidder shall pack or have packed the deliverables, as applicable: -

42.1 In accordance with DEFSTAN 81-041 (Part 1)/ STANAG-4280 or equivalent Military Standard.

42.2 To ensure that each deliverable may be transported in an undamaged and serviceable condition.

43. The Bidder shall ensure that each package containing the deliverable is labelled to include:-

43.1 The name and address of the consigner and consignee including:-

43.1.1 The delivery destination/ address if not of the consignee.

43.1.2 Transit destination/ address (for aggregation/ disaggregation, onward shipment etc).

43.2 The description and quantity of the deliverables.

43.3 The full part number in accordance with agreed codification details

43.4 The makers part, catalogue, serial, batch number, as appropriate.

43.5 The contract number.

43.6 Any statutory hazard markings and any handling markings including the mass of any package which exceeds 3 kgs.

43.7 The Packaging Label (military J, N or P, special H, commercial A, C etc) (specify reference to DEFSTAN 81-041 (Part 1)/ STANAG-4280 or equivalent Military Standard.)

44. **Monitoring of Project Based on Contractual Milestones/ PR *(as applicable)***. After placement of order, the progress of the project will be monitored by the Buyer for compliance with various activities towards achieving contractual milestones/ DPR involving delivery/ installation/ integration/ trials etc. The contractual milestones will be integral part of the contract. In case the project does not proceed as per the indicated timelines for various contractual milestone(s), the Buyer will have the right to invoke Termination of the project. The indicative list of Contractual Milestones broad range of timelines (earliest and latest time for completion) for the project is as follows (to be used for preparation of PPR and PR):-

Sl.	**Milestone**	**Timelines**	**Remarks**
44.1	Contract Conclusion	T0	**General**
44.2	Submission of Advance Bank Guarantee.	T0 + 15 days	**General**
44.3	Commencement of SRS discussions for ERP SAFAL.		**ERP**

	Handing over of sites by ICG		**Civil**
44.4	Submission of Project Report and Pert Chart.	T0 + 1 month	**General**
44.5	Submission of PBG.		**General**
44.6	Submission of blue prints/ building drawings for DC and DRDC buildings.	T0 + 45 days	**Civil**
44.7	Submission of list of clearances to be obtained by ICG.		**Civil Works**
44.8	Submission of DC/ DRDC blue prints/ building designs for uptime certification.	T0 + 2 month	**Certification**
44.9	Submission of application and documents for LEEDS certification for Green Building Norms.	T0 + 2 month	**Certification**
44.10	Placement of orders on Network Service providers.		**Network**
44.11	Placement of orders for all IT hardware (ERP, DC, DRDC, NLDR and ROBO racks for ships).		**Core IT infra**
44.12	Placement of orders for ERP licenses.		**ERP SAFAL**
44.13	Completion of design certification by uptime.	T0 + 3 month	**Certification**
	Submission of contract copy for civil works.		**Civil Works**
44.14	Commencement of civil works.	T0 + 4 month	**Civil Works**
44.15	Completion of excavation for foundation, PCC works in foundation up to plinth beam.	T0 + 5 month	**Civil Works**
44.16	Submit application for necessary certification/ clearance for underground fuel storage tank.		**Civil Works**
44.17	Completion of site survey and feasibility report of all network nodes.		**Network**
44.18	Finalisation of SRS documents for ERP SAFAL.	T0 + 6 month	**ERP SAFAL**

44.19	Delivery of ERP licences and Development Hardware for ERP.	T0 + 6 month	**ERP SAFAL**
44.20	Commencement of ERP development.		**ERP SAFAL**
44.21	Delivery and positioning of ROBO racks for ships		**IT infra(Ships)**
44.22	RCC columns upto roof level including lintel beam and roof casting of first floor.	T0 + 7 month	**Civil Works**
44.23	Commencement of Installation and Commissioning of ROBO Racks onboard ships		**IT infra(Ships)**
44.24	Commencement of establishing network links.	T0 + 8 month	**Network**
44.25	Completion of Installation and Commissioning of ROBO racks onboard ships		**IT infra(Ships)**
44.26	First Pilot implementation demonstration of ERP SAFAL/ MVCR in ICG network	T0 + 9 month	**ERP SAFAL**
44.27	RCC columns upto roof level including lintel beam and roof casting of second floor including roof treatment.	T0 + 10 month	**Civil Works**
44.28	Second Pilot implementation demonstration of ERP SAFAL/ MVCR.	T0 + 11 month	**ERP SAFAL**
44.29	Complete internal wiring and plumbing works.	T0 + 12 month	**Civil Works**
44.30	Delivery of all IT hardware (Core IT infra for DC, DRDC, NLDR and ERP production hardware).		**Core IT infra**
44.31	Commencement of Training for ICG personnel.		**Training**
44.32	Complete plastering (internal and external) and flooring works.	T0 + 13 month	**Civil Works**
44.33	Offer Testing/ Inspection of all IT hardware.		**Core IT infra**

44.34	Complete joinery works (carpentry).	T0 + 14 month	**Civil Works**
44.35	Certification/ clearances for underground fuel storage tank obtained.		**Civil Works**
44.36	Completion of establishment of all network links.		**Network**
44.37	Completion of finishing works (Painting, distempering etc.) including power backup and cooling of IT and non-IT area	T0 + 15 month	**Civil Works**
44.38	Provisioning of HT supply and water supply by ICG		**Civil Works**
44.39	Commencement of link testing		**Network**
44.40	Provisioning of fuel for Power backup		**Operations**
44.41	Completion of sanitary and electrical fitting and internal furnishing (creation of office space, common areas, provisioning of furniture's and desktop computers) of non-IT area.	T0 + 16 month	**Civil Works**
44.42	Completion of LEEDS certification for Green Building Norms		**Certification**
44.43	Completion of Testing/ Inspection of all IT hardware.		**Core IT infra**
44.44	Commence installation of all IT hardware (DC, DRDC, NLDR, Balance ROBO racks for ships and ERP production hardware).		**Core IT infra**
44.45	Offer the civil works for acceptance by ICG.	T0 + 17 month	**Civil Works**
44.46	Completion of all link testing.		**Network**
44.47	Offer ERP SAFAL for OEM audit.		**Audit**
44.48	Completion of Training for ICG Personnel.		**Training**
44.49	Offer civil works for construction certification by uptime.	T0 + 18 month	**Certification**
44.50	Completion of OEM audit of ERP SAFAL.		**Audit**

VERIFIED

44.51	Offer ERP SAFAL for security audit.	T0 + 18 month	**Audit**
44.52	Commissioning of all network links.		**Network**
44.53	Completion of Installations and Commissioning of all IT hardware (DC, DRDC, NLDR, Balance ROBO racks for ships and ERP production hardware).		**Core IT infra**
44.54	Place orders for hiring of technical onsite manpower.		**Manpower**
44.55	Positioning of ICG Manpower at DC & DRDC.		**Manpower**
44.56	Completion of construction certification by uptime.	T0 + 19 month	**Certification**
44.57	Offer the DC/ DRDC facility for Operation Certification by uptime.		**Certification**
44.58	Completion of security audit of ERP SAFAL.	T0 + 20 month	**Audit**
44.59	Forward final User Acceptance Trials (UAT) document for the entire project.		**Acceptance Trials**
44.60	Submit all licenses and codes in respect of ERP SAFAL and solutions deployed in DC, DRDC & NLDR.		**Licenses and Codes**
44.61	Submit all design specifications drawings, architectural drawings of civil infrastructure, OEM equipment manuals (Operations, Maintenance & Training) and Warranty & Guarantee Certificates.		**Documentation**
44.62	Completion of operation certification by uptime.	T0 + 21 month	**Certification**
44.63	Approval of final UAT document.		**Acceptance Trials**
44.64	Commencement of UAT.		**Acceptance Trials**
44.65	Forward details of on-site manpower to ICG.		**Manpower**
44.66	UAT.	T0 + 22 month	**Acceptance Trials**
44.67	Clearance for on-site manpower by ICG.		**Manpower**
44.68	Submit all Audit reports and certificates.		**Certification & Audit**

VERIFIED

44.69	Completion of UAT.	T0 + 23 month	**Acceptance Trials**
44.70	Position on-site manpower.		**Manpower**
44.71	Signing off project acceptance certificate.		**General**
44.72	Project Commissioning.	T0 + 24 month	**General**
44.73	Final go-live.		**General**
44.74	Submission of Warranty Bond Bank Guarantee by SI.		**General**

45. The Bidder is to indicate the proposed timelines for the above milestones in the Technical Bid. On conclusion of the Contract, these milestones will be monitored by the Buyer.

46. Considering the complexity of the Digital Coast Guard project, a Central Project Management approach will be adopted from the beginning through an Integrated Programme Management Group and Separate Dedicated Project Steering Groups for each component of the project. The constitution and functions envisaged for 'IPMG' are as follows:-

46.1 IPMG as an apex body shall provide single window clearance and vet all processes and activities associated with implementation of the 'Digital Coast Guard Programme'.

46.2 IPMG shall monitor the progress of project at every step and meet at periodic intervals to monitor the progress of the project and provide necessary guidance to the respective Project Steering Groups to accomplish the project timelines and objectives.

46.3 IPMG shall be headed by an officer of suitable seniority (IG or equivalent) and experience. Members should be drawn from the project team and concerned users directorates at CGHQ. External members from acquisition wing of MoD and other organisations may be co-opted based on the requirements.

47. Separate PSGs shall be constituted for one or more deliverables expected out of the framed objectives of 'Digital Coast Guard'. Each deliverable shall be managed at micro-level for compliance to the specified functional and technical requirements and adherence to the laid down timelines. Deliverables that do not involve the domain knowledge of other directorates/ agencies, shall be managed by Digital Coast Guard project team solely or in coordination with ICG Regions. The deliverables of the project, which may involve other user directorates shall be monitored and managed in consultation with the respective users/ agencies. Members from outside agencies could be co-opted in the PSGs based on requirements of specific domain expertise.

48. The Project Monitoring Meeting is to be organized at three (03) months interval during the first 12 months post conclusion of contract and thereafter at an interval of one month or as and when required. The Bidder shall attend the progress monitoring meetings through its Project Manager and shall submit progress reports to the Buyer.

The Project Manager assumes overall responsibility for the assignment and ensures that all resources required are made available and the engagement is carried out according to agreed plans. He shall function as the primary channel of communication for all ICG requirements to the implementation team. Other requirements are placed at **Appendix 'R'**.

49. **Change Management**. As per para 25 of Chapter-VIII of DAP-2020, SAFAL ERP and other ICT Application Enhancements (like software functionality enhancements etc) that are not conceived during the design stages, but are essential for successful utilisation of the application and those necessitated by change of policies of the Government/ Service Headquarters/ legislations and/ or due to change in the deployed techniques/ tactics by the adversaries may be progressed under Change in Service as under:-

49.1 **Deviations in Outputs/ Deliverables**. In cases of deliverables of the project needs to be enhanced due to certain strategic requirements posed by the dynamic nature of the environment, ICG will constitute an Empowered Committee for Change Control (ECCC) headed by an officer of the rank Inspector General. This committee will examine, evaluate and review the changes in service during project execution phase, deviation in deliverables/ outputs as mid-course corrections, accommodating minor variations in SQRs and need for upgradation of the project during its life cycle, after the finalisation of the contract, technology change, upgrades, additional integration and provision for any deviations in deliverables which are out of the initial scope of work, to be paid as Paid Change Requests to the Bidder as part of the main contract. The ECCC after assessing and evaluating the requirements of Change will recommend each case for approval. The proposals for each Change in software/ hardware or cumulative value amounting up to plus or minus 15% of the basic value of software/hardware for ICT projects and 10% of the basic value of System projects shall be approved under delegated power of ICG. Change proposals for each change value beyond the delegated power or cumulative value beyond plus or minus 15% (10% for Systems projects) of the basic value of software/hardware respectively shall be submitted for CFA approval.

49.2. **Accommodating Minor Variations**. Supply of higher specification products due to non-availability of same specifications as ordered may be accepted, provided the seller submits a certificate from the OEM that the ordered specifications of the product have been upgraded and there is no addition/ reduction in price.

PART-III - COMMERCIAL REQUIREMENTS

50. The third part of the RFP consists of the commercial clauses and Standard clauses of contract. The bidders are required to give confirmation of their acceptance of these clauses.

Commercial Bid

51. The Bidder is requested to take into consideration the *Commercial Clauses and Payment Terms* given at ***Appendix H*** to this RFP while formulating the Commercial Offers. The bidders are required to quote their price in Price bid format given in ***Appendix J*** to this RFP.

52. Commercial offers will be opened only of the Bidder who qualify the technical evaluation which includes pre-qualification criteria & compliance of technical specification. The Commercial Offer must be firm and fixed and should be valid for at least 18 months from the last date of bid submission.

Commercial Bid Opening

53. The Commercial Offers will be opened by the Contract Negotiation Committee (CNC) and if Bidder desires he may depute his representative, duly authorised in writing, to be present at the time of opening of the offers.

54. The date, time and venue fixed for this purpose will be intimated separately after the evaluations are completed.

55. The CNC will determine the lowest bidder (L1).

Additional Aspects

56. **Standard Conditions of RFP.** The Government of India desires that all actions regarding procurement of any equipment are totally transparent and carried out as per established procedures. The bidder is required to accept our standard conditions furnished at ***Appendix K*** to this RFP regarding Agents, penalty for use of undue influence and Integrity Pact, access to books of accounts, arbitration and clauses related to Law. These conditions along with other clauses of the Contract form the Standard Contract Document (as at **Chapter VI** of DAP 2020) indicates the general conditions of contract that would be the guideline for all acquisitions. The draft contract would be prepared as per these guidelines.

57. **Option Clause** The option clause is limited to procurement of hardware, ROBO, network components and ERP licenses*.* The format of option clause is placed at **Appendix L** to this RFP.

VERIFIED

PART III BID EVALUATION AND ACCEPTANCE CRITERIA

58. A list of documents/ details to be submitted along with the bids is placed at **Appendix O** as a reference to help in completeness of bid and meeting the procurement process schedule.

59. The bids shall be unconditional and unqualified. Any condition or qualification or any other stipulation contained in the bid shall render the bid liable to rejection as a non- responsive bid.

60. The bid and all communications in relation to or concerning the bidding documents shall be in English language.

61. **Evaluation and Acceptance Process.**

61.1. **Evaluation of Technical Proposals**. The technical proposals forwarded by the Bidders will be evaluated by a Technical Evaluation Committee (TEC). The TEC will examine the extent of variations/ differences, if any, in the technical characteristics/ parameters of the equipment and ERP solution offered by various Bidders with reference to the QRs placed at ***Appendix 'A'*** and prepare a "Compliance Statement" for shortlisting the Bidders.

61.2. **Evaluation of Commercial Bid**. The Commercial bids of only those bidders who qualify in the TEC will be opened. Comparison of bids would be done on the basis of evaluation criteria given in ***Appendix J*** to this RFP. The L-1 bidder would be determined by Contract Negotiation Committee (CNC) on the basis of- ***Appendix J*** to this RFP. Only L-1 bidder would be invited for negotiations by CNC.

61.3. **Contract Conclusion/Placement of Order *(as applicable).*** The Successful conclusion of CNC will be followed by contract conclusion/ placement of order.

Appendix A
{Refers to Para 26, 27, 28, 30.1, 31, 36 & 61.1 of RFP and Para 8 of Appendix 'C'}

OPERATIONAL CHARACTERISTICS AND FEATURES

TECHNICAL SPECIFICATIONS: DATA CENTRE

Introduction

1. The Data Centre (DC) & Disaster Recovery Data Centre (DR DC) is home to the computational power, storage, and applications necessary to support IT requirements to meet the objectives of Digital Coast Guard which includes Coast Guard administrative, surface/air logistics, technical and operational activities. The Data Centre infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the DC infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered. Important aspect of the DC design will be its flexibility to quickly deploy and support new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant advantage. Such a design requires robust initial planning and thoughtful consideration in the area of port density, access layer uplink bandwidth, true server capacity, and oversubscription, to name just few. Data centre should be designed and built to meet the standards of Tier-3 by Uptime Institute.

2. The DC design need to be based on a proven layered approach, conceptually which has been tested and improved over the past several years in some of the largest data centre implementations in the world. The layered approach is the basic foundation of the data centre design that seeks to improve scalability, performance, flexibility, resiliency, and maintenance. Some of the key objectives of the Data Centre are: -

2.1. Optimal Utilization of space

2.2. Higher availability of system and data

2.3. Scalability in phased manner

2.4. Designed as per Tier-3 guidelines

3. Only the **clear land** will be provided by Coast Guard to the SI for construction of civil infrastructure for the Data Centre. The SI has to establish the data centre as per standard and involve Uptime Institute right from inception till final certification for complete project. The DC shall be designed catering for following: -

3.1. **Scalability**. DC shall be designed so that capacity be scalable enough for catering to the need of user, data or application growth in future within the same footprint of initial proposal. The quality of the scalability will be judged by the capability of the system to make available the resources in the simplest and quickest manner, with minimum or avoiding manual intervention. Following scalability requirements will be factored in, but not be limited to, the design criteria of DC:-

3.1.1. Total IT equipment load of 170 Kw Scalable up to 200% (34 Racks of 10 Kw Each).

3.1.2. DG Set in N+N configuration as required and the design of the DC should cater for scalability up to 200%. Provisioning of DA include installation & commissioning.

3.1.3. Double Conversion Online modular UPS system in N+N configuration should be provided for the DC. Batteries of Lithium-ion type be provided to support a backup time of 10 minutes.

3.1.4. The cold aisle containment with perimeter cooling solution should be provided.

3.1.5. The Phase wise minimum required capacities for the proposed DC shall be as follows:-

Sl.	**Equipment**	**Total Capacity Required**	**1st Phase Requirement**	**2nd Phase Requirement**
3.1.5.1	Transformer	750 KVA (N+N)	-	-
3.1.5.2	DG Set	800 KW (N+N)	400 Kw X 2NOS	400 Kw X 2NOS
3.1.5.3	DG Sync Panel	750 KW (N+N)	1	NIL
3.1.5.4	LT Panel	750 KVA (N+N)	1	
3.1.5.5	Modular UPS	400 KW(1+1)	200 Kw Modules + Chassis	200 Kw Modules
3.1.5.6	With Lithium Lion Battery	10 Minutes Backup	X 2 NOS	X 2 NOS
3.1.5.7	PAC	108 TR	27 TR x 3 No (N+1)	27 TR x 2No (N+1)

3.2. **High Availability**. Availability is best defined as the time an application and the system resources are available to the user on 24x7x365. This is implemented through hardware, software and services. Adequate redundancy at various levels of DC is one of the ways of gaining high availability and should be provisioned in order to ensure availability various applications, database and services. The approach to achieve this design objective can be categorized as follows:-

3.2.1. Dual-Raw Power Supply

3.2.2. Modular UPS Power Supply system in N+N configuration.

3.2.3. Cooling system in N+1 configuration

3.3. **Interoperability**. The nature of the server room creates an intense need to have access to multiple OS platforms, which aid in application deployments, migrations and updates. Hence, there is a need to accommodate multiple OS platforms within the network, either on one system or multiple systems. Interoperability is an important design parameter, especially for selecting the Storage solution. Storage has to be interoperable with the Servers, HBA, Tape Solution and Backup and Archival Solution.

3.4. **Maintainability**.

3.4.1. Ability to perform routine maintenance without affecting mission critical operations

3.4.2. Online monitoring of infrastructure system

3.4.3. Information system with key specifications and operating instructions

3.5. **Redundancy**.

3.5.1. Considerations on secondary components becomes vital in the event of a primary component failure.

3.5.2. Elimination of single points of failure wherever feasible.

3.5.3. Redundancy of N+1 for Cooling system, N+N for UPS, Dual-Feed of raw power supply circuits etc.

3.6. **Security**.

3.6.1. Protection from security breach and man-made threats.

3.6.2. Well defined security policies.

3.6.3. Mix of physical and electronic security measures.

3.7. Centrally managed & monitored data centre facility infrastructure & IT infrastructure. Vendor to provide Data Centre Infrastructure Management (DCIM) tools monitor, measure, manage and/or control data centre utilization and energy consumption of all IT-related equipment (such as servers, storage and network switches) and facility infrastructure components (such as power distribution units [PDUs] and computer room air conditioners [CRACs]).

3.8. **Hierarchical Networked LAN**. It shall use a two-tier collapsed core network architecture that combines the core layer with the aggregation layer. Data Centres contain centralized computing resources vital to all personnel in the organization, be they at headquarters, a large regional office or at a remote branch office. As most critical business processes are carried out online, any Data Centre LAN downtime or inefficiency has a negative impact on business processes and the organization bottom line. The Data Centre LAN must provide secure, high-performance, high-available LAN services at scale to ensure that the network is always online and that the necessary resources are always available to maximize business productivity and customer satisfaction.

3.9. **Integration and Migration of Data**. Vendor should implement the private cloud for buyer and implement the functional requirements fully with the supplied and existing hardware/ software (***Annexure I & II***) i.e., integration with manager of the hypervisor, Software Defined Network and storage, etc. Migration of data in the new system is responsibility of the bidder. ICG along with bidder will jointly decide on what data will be migrated and will take the responsibility of collecting and making the data available in digitized form as per the format suggested by the bidder. A detailed plan for data migration is expected from the bidder during the initial stages of the project, which will include data to be migrated, templates for upload of data and data collection/digitization/migration timelines.

4. **Design Sizing**. The clear land will be provided to bidder by ICG. The bidder has to construct the civil infrastructure for approximately 3035 Sq. mtr carpet area (Average floor area for G+2 with stilt area of 1012 Sq Mtr) for data Centre. Data Centre design should be certified for meeting Tier-III standards by Uptime Institute and relevant certificate to be provided. For that the bidder shall have to involve the Uptime Institute right from design, layout, construction till final handing over of the civil infrastructure. The average power consumption for each server rack to be considered is 10 kW. Further scalability of the building should be considered while designing of Data Centre.

5. **Scalability**. Considering the high probability of exponential growth in IT requirements for ICG, it is preferred to cater additional equal capacity of IT load scalability option on exhaustion of present designed capacity and required building foundation, structural designing to cater for expansion of further 02 floors in future. Accordingly, additional load-bearing floor equal to present Server & Utility Area may be provisioned and required ground space may earmarked. For better utilization of additional space, it may be used to cater for non-essential requirements such as car parking, landscape etc.

6. **Scope of Work**. The Data Centre should follow the guidelines of Tier-3 data centre containing essential elements. The entire cooling, power and other facilities should support DCIM for centralized monitoring & management. The scope of work consists of supply and installation of the following:-

6.1. Layout diagram/ Architectural diagram of the building to be provided by the bidder to ICG within 45 days of signing of contract.

6.2. Data centre civil and interior infrastructure as per the Designated Area Size. Data centre design should be certified for meeting Tier-III standards by Uptime Institute and relevant certificate to be provided.

6.3. The Complete Electrical Infrastructure from Feeder to the Critical Load including HT, LT with BBT required to operate and manage the complete DC with respect to equipment and manpower required for this DC.

6.4. The manpower should be planned for 5 years from the date of acceptance.

6.5. All the equipment supplied should have two years warranty plus 3 years comprehensive AMC cost included in the offered proposal.

6.6. High density server racks and network racks be provided.

6.7. The air-cooled based HVAC solution for the entire building should be offered.

6.8. High density DX based perimeter cooling system in N+1 configuration

6.9. Software Defined Data Centre (SDDC) enabled servers, storage and networking devices including virtualization, clustering, etc.

6.10. Integrated Data Centre Infrastructure Solution with complete IBMS & DCIM should be provided.

6.11. 120 workstations or as required.

6.12. Magnetic Whiteboards (1200x2400mm).

6.13. Video Wall for 24x7 monitoring, super Narrow Bezel LED Display, 24x7 rated, 30′ x 10′ in tile configuration with accessories for "Command Centre" and 20′x10′ for Security Operations Centre (SOC).

6.14. AV Solution for all the meeting & Conference room with VC Capability should be provided.

6.15. Life safety and security systems with following facilities:-

6.15.1. Fire Detection/alarm & Fire suppression system (Novec 1230 Gas)

6.15.2. Public Address System

6.15.3. VESDA as per uptime tier III certification

6.15.4. Access control with visitor management system

6.15.5. CCTV system

6.15.6. Rodent repellent system

6.15.7. Water leakage detection system

6.15.8. Environmental monitoring system (EMS)

6.15.9. Hydrant Based Fire Fighting System

6.15.10. Integrated Perimeter Security should be provided

6.15.11. Retractable Bollards

6.15.12. Baggage Scanners & Metal Detectors

6.15.13. Under Vehicle Scanners

6.16. Office area furnishing (Interiors)

6.17. Other Building Services like WTP, STP, Rain Water Harvesting, HSD Yard, DC Building Related Landscaping

7. **Specification**

7.1. **General specifications**. The data Centre should follow the guidelines of Tier-3 data Centre containing essential elements.

7.2. **Civil & Interior works**. Data Centre civil and interior infrastructure as per the enclosed layout. The outer elevation and colour of the building should be designed in consultation with ICG.

7.3. **Specification of FS 800 HPL Panel/Tile**

Tile Size	-	600mmx600mmtile
Tile thickness	-	35mm
Module	-	FS-800(HDG-6008HPL)
Point Load	-	450 Kg.
Uniform Dis. Load (UDL)	-	2000 Kg. per M2
Height of Pedestal	-	750mm

7.4. **Finish**. Top covering with high pressure antistatic hot-pressed laminate 1.00mm thick, factory finish in universal white colour and grey streamlet pattern. Edge bonded with black conductive PVC beading.

7.5. **Tile**. All steel construction & cavity filled with epoxy mix cement. Top plate 0.70, Bottom plate 0.70mm of steel with grey colour powder coated on a continuous line having 64 round embossing to the bottom plate with 100 spot welding to weld top & bottom plate.

7.6. **Pedestal**. All steel constructions & yellow Zinc plated 25mm Dai pipe pedestal with bottom plate of 100mm x 100mm x 2mm thick. Top plate of 75mm x 75mm x 3mm thick with threaded bolt & 2 nuts for levelling adjustment.

7.7. **Stringer**. Stringers of 0.80 mm thick rectangular pipe of size - 20mm (W) x 30mm (Ht.) x 573 mm long, 2 holes centre to centre 550 mm. Special feature of the Product:

7.7.1. Factory finish laminates.

7.7.2. Conductive edge beading.

7.7.3. Solid concrete field, higher load bearing capacity.

7.7.4. Special weather coating on back surface of the tiles.

7.7.5. Totally fire proof.

7.7.6. Fast & accurate installation.

7.8. **Mode of measurement**. Any cut plate up to 300mm width will be charged as 300mm width for measurement & cut plate above 300mm width will be charged as full plate (600mm). No deduction shall be given for any opening & cut outs.

7.9. **Fire Rated Doors**

7.9.1. Door leaf Single/Double shall be 46mm thick fully flush double skin door with vision panel of 300 x 300 mm size fitted with fire rated glass. Door leaf shall be manufactured from 1.6 mm minimum thick galvanized steel sheet Fe 355 grade (not re-rolled). The internal construction of the door should be rigid reinforcement pads for receiving appropriate hardware. The infill material shall be resin bonded honeycomb core. Fully flush, double skin door shell with lock seam joints at stile edges. Internal reinforcements shall be provided at top, bottom & stile edges for fire rating.

7.9.2. Hinges are to be provided of SS 316 grade Stainless steel double ball bearing butt hinges of size 100mm x 76mm x 3mm thick conforming to BS 7352 standard for 'Strength and durability performance of metal hinges for side hanging applications and dimensional requirements for template drilled hinges' and are classified in class 8 i.e., with 20000 annual operations. The screws for hinges shall be SS 316 grade Philips head CSK screws of size M6x 15mm.

7.9.3. All fire doors must be hung on minimum four no steel hinges, to resist bowing in the event of a fire and to bear the increased weight of the door.

7.9.4. Fire resisting doors must be fitted with external dual action hydraulic type self-closing devices which are adjusted to close quickly but latch slowly so as not to wear the smoke seals or damage the door or frame. Perco-type closers are not suitable as they cause the doors to slam causing noise nuisance to occupiers and they tend to wear the smoke seals/frames causing damage over a period of time. Self-closers are to be attached using appropriate fixings („snake eye screws") which are designed to prevent removal/tampering by user.

7.9.5. All doors and frames shall be suitably cleaned and primed with two component epoxy primer and finished with polyurethane aliphatic grade paint of approved colour. The door leaf and frame shall have passed minimum 500 hours of salt spray test.

7.9.6. Door Accessories shall be similar fire rating as of Doors.

7.9.7. The fire Doors with frame shall be as per IS: 3614 part 4 and BS: 476 part 20, and tested at FRL CBRI Roorkee or ARAI with standard heating conditions as specified in IS: 3809 - 1979 and BS: 476 part 20 & 22 1987 all complete to the entire specification with the certified copy of the valid Test Certificates to be issued by OEM.

7.10. **Door Frame Metal Detector**. These are security gates used for the entrance automation to provide high security at the inner premises. These gates are highly recommendable for entering and exiting in government offices, malls, airports, metro stations, etc. Features are as follows:-

7.10.1. Its performance is good, and failure rate is low.

7.10.2. Door with LED and 6 Zone detection points.

7.10.3. Anti-inference with location signal display light.

7.10.4. Using PVC composite material which is waterproof and fire proof.

7.10.5. Synchronous sound and light alarm.

7.10.6. Big LCD Screen with English operation system.

7.10.7. Easy assembly. Technical specification are as follows:-

Outer frame	2200x800x550 (mm)
Inner frame	2000x700x550 (mm)
Sensitivity (adjusted)	0-255
Power Supply	90-240 V (AC)
Power consumption	20 W Aprox.
Working temperature	-20°C to 65°C

8. **Electrical & UPS works**.

8.1. **UPS Specifications.**

8.1.1. 200 kVA modular UPS in N+N configuration, scalable up to 500 KVA and Lithium-ion Battery banks to provide minimum 10 minutes back up at full load. Should be integrated with DCIM software for centralized monitoring & management.

8.1.2. The UPS should be the latest state-of-the-art modular system and shall be a single unit, complete with modular, parallel redundancy with Lithium-ion batteries. UPS standards like EN 62040-1:2008, 2011 and 2013 must be followed.

8.1.3. The capacity of the UPS system proposed should take care of server, network, storage and lighting load along with safety margin.

8.1.4. It should be configured in N+N redundancy mode.

8.1.5. The power modules shall be hot-swappable and while the system is running live, removing or replacing power modules shall have no impact on the load. It should be possible to add or replace power modules without switching the load to bypass source. Notification should be provided on the UPS integrated display for add or removal of Power module.

8.1.6. The main system controller shall be hot-swappable and while the system is running live, removing or replacing the main system controller shall have no impact on the load.

8.1.7. The UPS system shall be upwardly scalable by simply adding UPS power modules to the available shelves, and adding more shelves if required with no need of any additional parts.

8.1.8. UPS shall be provided with BMS interface and integrated with unified IT Operations Management software for centralized management & monitoring.

8.2. **Battery specification as following**.

8.2.1. Lithium-ion of NMC type

8.2.2. Sealed maintenance free batteries

8.2.3. Battery Protection using Electronic switch (SCR) & Fuse

8.2.4. Battery housing should be compact and space saving MS steel open racks complete with interconnectors/ Battery fuse box or isolator (in case of external protection) - IP 20.

8.2.5. Mounted in a rack.

8.2.6. The UPS battery shall support replaceable, hot swappable, fused, battery modules.

8.2.7. Each battery module shall be monitored for voltage and temperature for use by the UPS battery diagnostic. Battery charging current shall be temperature compensated.

8.2.8. The UPS shall incorporate a battery management system to continuously monitor the health of each removable battery module. This system shall notify the user in the event that a failed or weak battery module is found.

8.2.9. The Batteries shall be long life batteries (05 years)

8.2.10. Battery recharge/ Certification:-

8.2.10.1. The battery offered shall re-gain its 100% power in 2 hour to 4 hours or less.

8.2.10.2. Certification for Li-Ion battery: UN38.3, UL1973

8.2.10.3. Built-in CMU (Cell Management Unit) to monitor individual cell voltage, temperature and manage cell balance.

8.2.10.4. Built-in isolated CAN Bus among CMUs & BMU for high voltage battery string operation.

8.2.10.5. Operating range for battery without deration in battery capacity - 0°C to 45°C.

8.3. **Electrical Panel and Distribution**. Electrical Panel and Distribution shall consist of minimum of following:-

8.3.1. The Data Centre main panel will be located in appropriate room and this will distribute the power to the UPS and other utilities.

8.3.2. Required number of PDUs in redundancy.

8.4. **Earthing**. "Maintenance Free Earthing", which uses special highly conductive backfill in place of conventional salt/ charcoal should be provided for all equipment's protective earthing. Earthing standards such as IS:3043-1987, IEEE 80:2012 & IEC 62561- 7:2018 must be followed.

8.5. **Lighting and Raw power distribution**.

8.5.1. Lighting to be designed for the illumination level of 500 lux at server room and 300 - 350 lux at UPS room.

8.5.2. Light fixtures shall be ceiling/ recess mounted type

8.5.3. Emergency lighting circuits shall be done to maintain required visibility in case of emergency/main power failure.

8.5.4. Separate DB should be provided which will distribute the power to emergency lighting, Fire and safety security system.

8.5.5. Required number of raw power sockets shall be provided for utility purpose, IT Office area and NOC area.

8.6. **Cooling works**. Data Centre cooling solution should be perimeter cooling solution with 42U useable rack space per rack to support Medium/ High Density Rack Load of up to 10KW per rack. The Cooling units should be in (N+1) configuration.

8.6.1. Data Centre cooling solution should be deployed in phased manner with all required Racks supplied in one go.

8.6.2. All Electrical and piping work for cooling solution for all phases to be completed in Phase-I. Cooling units will be added as required in the later time for Phase I & II.

8.6.3. Suitable Monitoring software to be provided for monitoring the complete health of the cooling solution

8.7. **Centralized integrated building air-conditioning**. Entire built-up area of data Centre should be centrally air-conditioned using VRV/ VRF Solution. Should be enabled for centralized monitoring using IBMS software. Should comply fully with latest edition of IS 659:1964 standards.

8.8. **Fire, Safety & Security Systems**.

8.8.1. **Access control system**. It is required to install an electronic access control system that allows only restricted access to different areas based on pre-set access policy. It also logs the entry and exit for auditing later. This system assists in controlling any unauthorized movement within:-

8.8.1.1 Server Room using card and biometric reader with single person interlock system (to prevent piggy backing).

8.8.1.2. UPS and Electrical room using card reader.

8.8.1.3. NOC, Telecom room, BMS room using card reader.

8.8.1.4 Generator area and data Centre perimeter area using intrusion detection system.

8.8.2 **CCTV system**. The primary objective of a CCTV system is to ensure effective 24x7 surveillance of an area and also create a record for post event analysis for 30 days.

8.8.2.1 Server room, generator area, parking, telecom, NOC, BMS and UPS room shall be covered using high resolution, fixed dome camera Closed Circuit Video Surveillance.

8.8.2.2 Perimeter Security using CCTV.

8.8.2.3 All CCTV cameras should be IP, PoE enabled and comply to ONVIF standards.

8.8.3 **Fire Detection, Alarm System**. The Conventional fire alarm system with multi sensor detector will be connected to the fire alarm control panel through a pair of wires. Manual call points to be provided to trigger the alarms manually in case of emergency situations and also strobes cum hooters are to be provided to give the alarms with sound as well as strobe indications. The panels are modular in nature and can be customized to the specific requirement by selecting the suitable housing, rail and modules. The panels are configured based on the requirement. The conventional fire alarm system to consist of the following systems at different areas of the Data Centre as mentioned below:-

8.8.3.1. Fire alarm control Panel

8.8.3.2. Manual call point

8.8.3.3. Strobe cum sounder

8.8.3.4. Heat detector for UPS room

8.8.4. **Fire Suppression System**.

8.8.4.1 The bidder shall supply, install, test and put in operation NOVEC 1230 based fire suppression system. The fire suppression system shall include and not be limited to gas release control panel, seamless cylinders, discharge valve (with solenoid or pneumatic actuator) as the case may be, discharge pipe, check valve and all other accessories required to make a complete operation system meeting applicable requirements of NFPA 2001 standards and installed in compliance with all applicable requirements of the local codes and standards.

8.8.4.2. The system design should be based on the specifications contained herein, NFPA 2001 and in accordance with the requirements specified in the design manual of the agent. The bidder shall confirm compliance to the above along with their bid.

8.8.4.3. Complete Pipe work, cabling and relevant installation should be catered for entire server room IT infrastructure.

8.8.4.4. Hand held fire extinguishers shall be provided at NOC/ office area and UPS room as follows:-

8.8.4.4.1 4.5Kg Clean Agent ABC type portable fire extinguishers for UPS Room/ BMS/ TELCO Area.

8.8.4.4.2 ABC Stored Pressure type Fire Extinguisher 6 Kgs for NOC/ Office area.

8.8.4.4.3. Foam soda Extinguishers for DG Area.

8.9. **Water Leak Detection and Rodent Repellent**.

8.9.1. Tape sensor cables to be provided to detect water leak or flooding. Water leak will cause contact closure in the cable circuit to send an alarm through Panel locally and through BMS to concerned.

8.9.2. Rodent repellent shall have master control unit with satellite modules on at least 6 variable frequencies to change alternatively which will be located at strategic location and with variable frequency ultrasound to deter the rodents that inhibit the server room.

8.9.3. The Rodent Control System should withstand high temperature fluctuations and should not cause any sparking.

8.10. **Environmental Monitoring System**. Environmental Monitoring system should be able to monitor the Temperature, humidity in the server room and UPS room environment.

8.10.1. It should be capable to measure temperature and humidity in each rack.

8.10.2. IP based and be able to monitor from remote through BMS.

8.10.3. It should be capable to integrate with building management system.

8.10.4. It should be rack mountable type.

8.11. **BMS and NMS Systems**.

8.11.1. The Building Management System will be implemented to monitor the various systems installed later. Entire server room, Equipment should be monitored with the DCIM and Unified IT Operation Management with Network Management System (NMS). All Data Centre components should be provided with suitable DCIM/ BMS/ UIM interface modules. All required cables and relevant accessories to be laid. Detailed specification of DCIM and BMS are given in Chapter 06 of DPR.

8.11.2. IP enabled PDU compatible to BMS with the following design:-

8.11.2.1. Sleek design.

8.11.2.2. Locking power chord.

8.11.2.3. Temperature/ humidity sensor compatibility.

8.11.2.4. Ability to generate threshold value to generate e-mail alert.

8.11.2.5. Ability to generate data reports of temperature/ humidity/ ampere/ kw/ kwh.

8.11.2.6. BMS will be capable of monitoring each cooling system, UPS, Electrical Panels and complete security system such as Fire alarm system, fire suppression system, EMS, ACS, VESDA, WLD, etc.

9. **Software Defined Data Centre (SDDC) enabled Server, Server Chassis, Software, Main Storage and Backup Tape Storage Systems with Application Delivery Controller (ADC)**. Detailed sizing and technical specifications are given in Chapter-06 of DPR.

10. **Installation and Support**. Following minimum support shall be provided:-

10.1. Installation support for all related software, hardware, networking, storage configuration including latest Windows Active Directory, Virtualization, Live migration of VM, Clustering support, Application Virtualization Clustering, Backup, Archival & Restoration and User/ Administrator setup.

10.2. Training material including step-by-step configuration Operating/ Maintenance procedures.

11. **Fuel System**. Design architecture of fuel system must be in accordance with Tier-III data centre standards. The path of fuel supply and return lines must be either concurrently maintainable or fault tolerant. The fuel system components namely pumps, manual valves, automated valves, control panels and tanks must meet either the concurrently maintainable or fault tolerant objective. All piping inclusive of fittings and valves shall follow the applicable BIS codes. Specification of pipe, pipe fittings and valves are enumerated below:-

11.1. Pipes shall be MS class 'C'& fittings shall be welded type fittings conforming to relevant BIS codes. All jointing in the pipe system shall generally be by welding/ flanges unless otherwise mentioned or directed at site.

11.2. All pipes and their steel supports shall be thoroughly cleaned and given on primary coat of red oxide paint before being installed. All welded piping shall be subject to the approval at site.

11.3. Thread joint fittings shall be malleable casting of pressure rating suitable for the piping system.

11.4. Tee-off connections shall be through equal or reducing tees other-wise ferrules welded to the main pipe shall be used.

11.5. Flanges shall be approved make. The supply of flanges shall also include supply of bolts and nuts and suitable asbestos fibre/ rubber insertion gaskets (minimum 3 mm thick).

11.6. Swing check valves shall normally be used in all services. Lifts type valves may be used in horizontal runs.

11.7. The strainers shall be of cast iron body with gunmetal or bronze mesh for fine filtration of the oil.

11.8. All piping and fitting shall be pressure tested, then painted and shall be provided with additional weather proof treatment for buried pipes.

11.9. Supply of diesel to Day oil tank from the bulk oil storage tank shall be automatically controlled by providing level sensor on each tank and controlled by Solenoid valves. Single pipe line shall feed to number of tanks.

11.10. System shall be provided to return the diesel fuel automatically back to the bulk storage tank in the case of pump supplying diesel from the bulk storage tank to the Day oil tank over runs. Pump capacity and Head shall be worked out by the vendor on the basis of Site condition.

12. **Miscellaneous**.

12.1. **Glow Signage**. Glow signage on both sides of the door shutters marking PUSH/ PULL along with other signage marking for different work areas and emergency signs.

12.2. **Shoe Rack**. Shoe rack to be provided at the entry of server room to avoid entry of dust in to the server room.

12.3. **Name Plate**. Suitable aesthetically designed brass name plate containing “Data Centre" to be affixed in the entrance, Electrical room, First Aid Box, Shock treatment chart, Emergency Rescue Instruction chart and insulated gloves for Electricians.

12.4. **Work stations**. 120 work stations of data centre specification to be provisioned in DC. Cabin to cubicle ration is 20:80. Size of the cabin - 10'x15' and cubicles - 8'x6'. Each cabin/ cubicle to be equipped with one Desktop computer (minimum i7 or equivalent processor, RAM- DDR4 8 GB & Storage 1TB, 22” LED Monitor, 1 KVA UPS). DC to be provided with 04 Heavy Duty MFDs and 15 printers each (05 color and 10 BW).

12.5. **Work space amenities**. Data Centre to be provisioned with Common area, Conference Rooms, Terrace Open Area, Store Rooms, wet canteen, Dining Space, Restrooms, Lobby and Lounge with adequate furniture.

12.6. **Parking space**. Parking space should be able to accommodate 80 four wheelers and 70 two wheelers.

12.7. **Industrial RO plant and portable water dispensers**. Data centre to be equipped with one industrial RO plant (Minimum 250 Ltr/ Hour capacity). Two heavy duty water dispensers to be provisioned in each floor with direct connectivity from RO plant.

12.8. **Lightening Arresters**. Lightening protection system complying with recognized safety standards of LPI175, NFPA780 and UL96A to be installed in the data Centre to avoid downtime, outage and service interruption caused by the after effect of Lighting.

13. **High level of Bill of Material**.

Sl.	Item description	Qty	UOM
13.1	DC Civil, Electrical and Interiors	1	Set
13.2	DC In-Row Cooling Solution	1	Set
13.3	Centralized Integrated Building Air conditioning	1	Set
13.4	Modular UPS as per above defined capacities with Lithium-ion batteries for server room	2	Sets
13.5	Fire Alarm & NOVEC 1230 based Gas Suppression System	1	Set
13.6	Rodent Control System	1	Set
13.7	Water Leak Detection System	1	Set
13.8	BMS & DCIM Software & Accessories (Complete Solution as required)	1	Set
13.9	Environment Management System (EMS) & Accessories (Complete Solution as required)	1	Set
13.10	Biometric Door Access System (as required)	1	Set
13.11	IP Dome Surveillance Camera (as required)	1	Set
13.12	Portable Fire Extinguisher (as required)	1	Set
13.13	DG Set 320KVA with AMF	2	Nos.
13.14	Server Racks of 10 KW capacity	34	No.
13.15	VESDA	1	Set
13.16	IT infrastructure sizing and detailed technical specifications as per Chapter-06 of RFP/ IT infrastructure detailed technical specification	1	Set
13.17	Video Wall for 24x7 monitoring, Super Narrow Bezel LED Display, 24x7 rated, 4 x 55" in tile configuration with accessories	1	No.
13.18	Media Safe	1	No.
13.19	Workstations alongwith one Desktop computer (minimum i7 or equivalent processor, RAM- DDR4 8 GB & Storage 1TB)	120	No
13.20	Structured Cabling	1	Set
13.21	Antivirus Software solution	1	Set

14. **<u>Suggested DC Layout - Ground Floor (The Bidder may submit proposed design for approval).</u>**

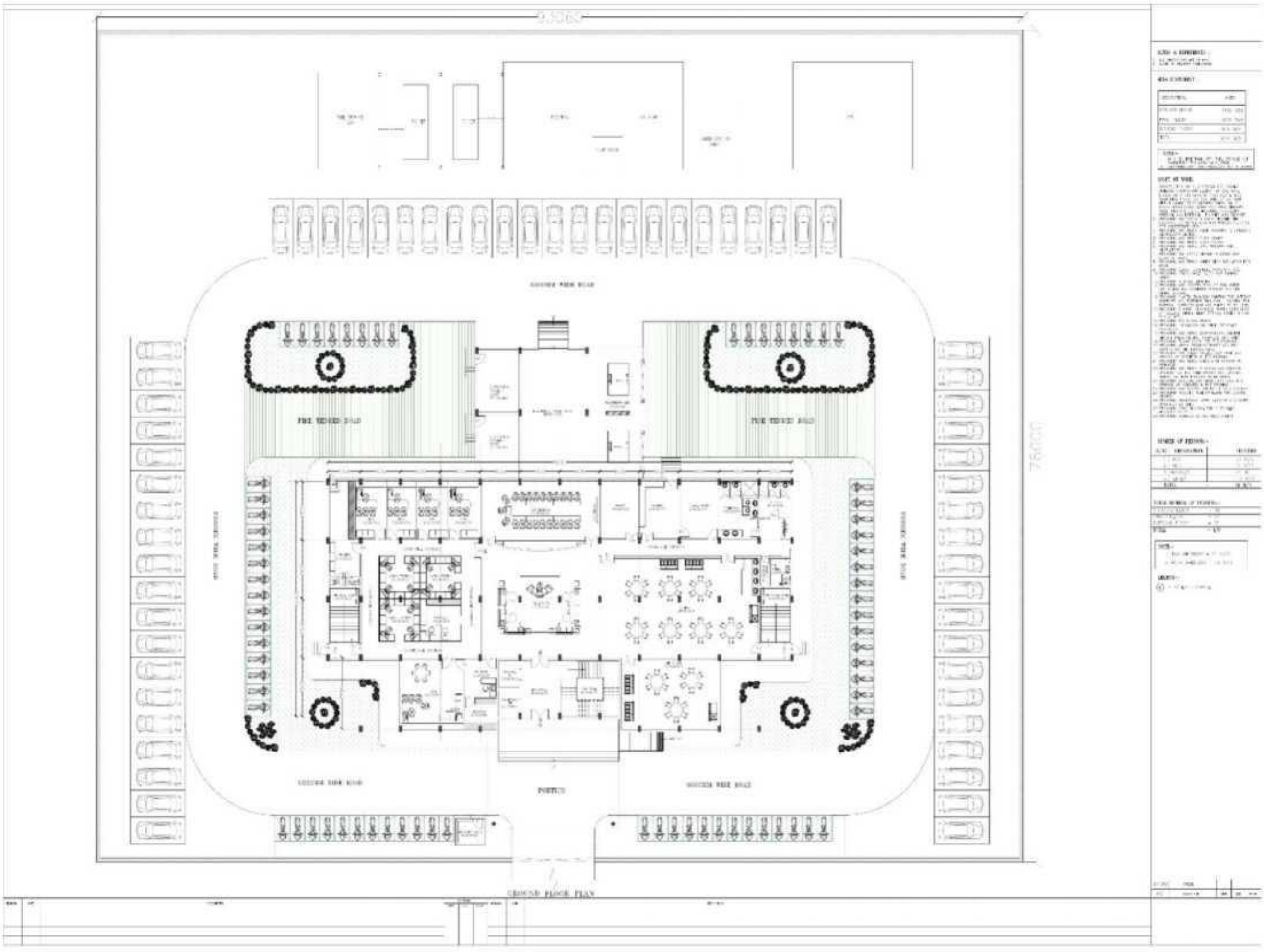
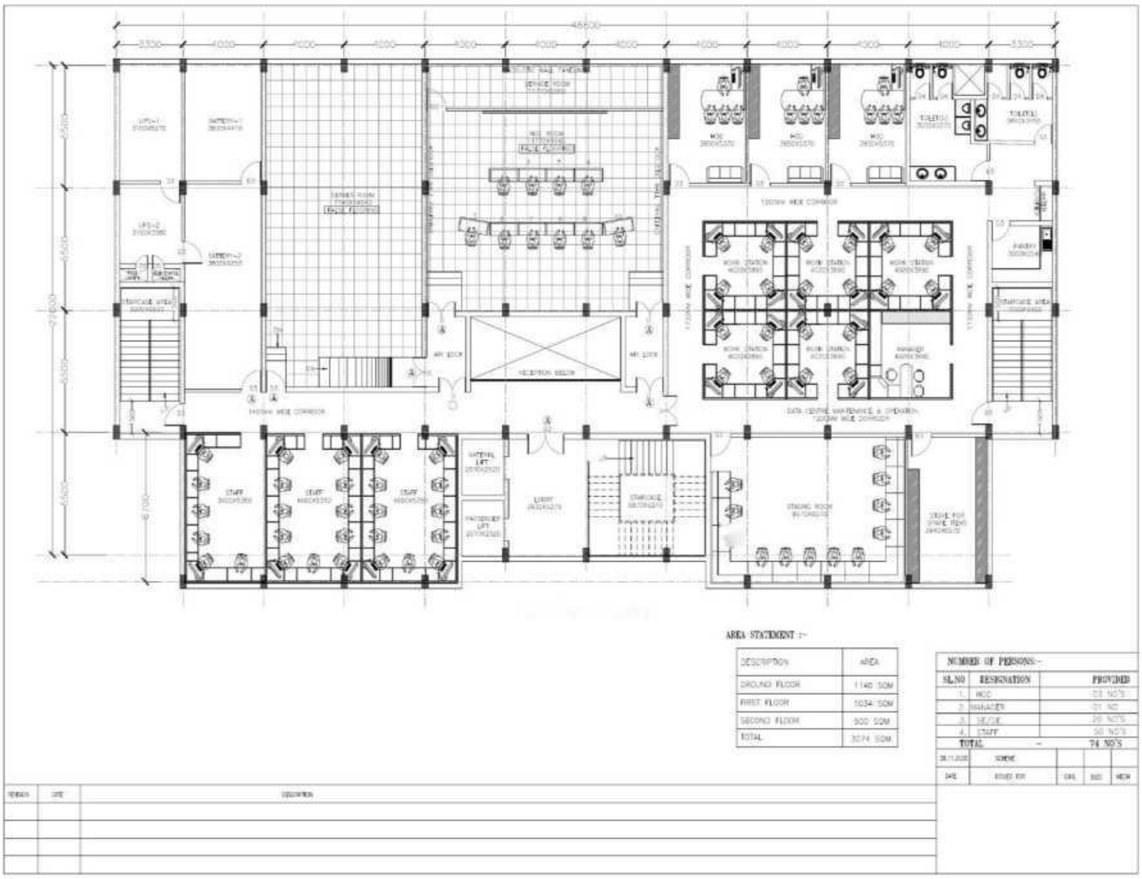


Figure 3-A: Primary DC - Physical Layout (Required)

<u>*VERIFIED*</u>

15. **Suggested DC Layout - First Floor (The Bidder may submit proposed design for approval).**



AREA STATEMENT :-

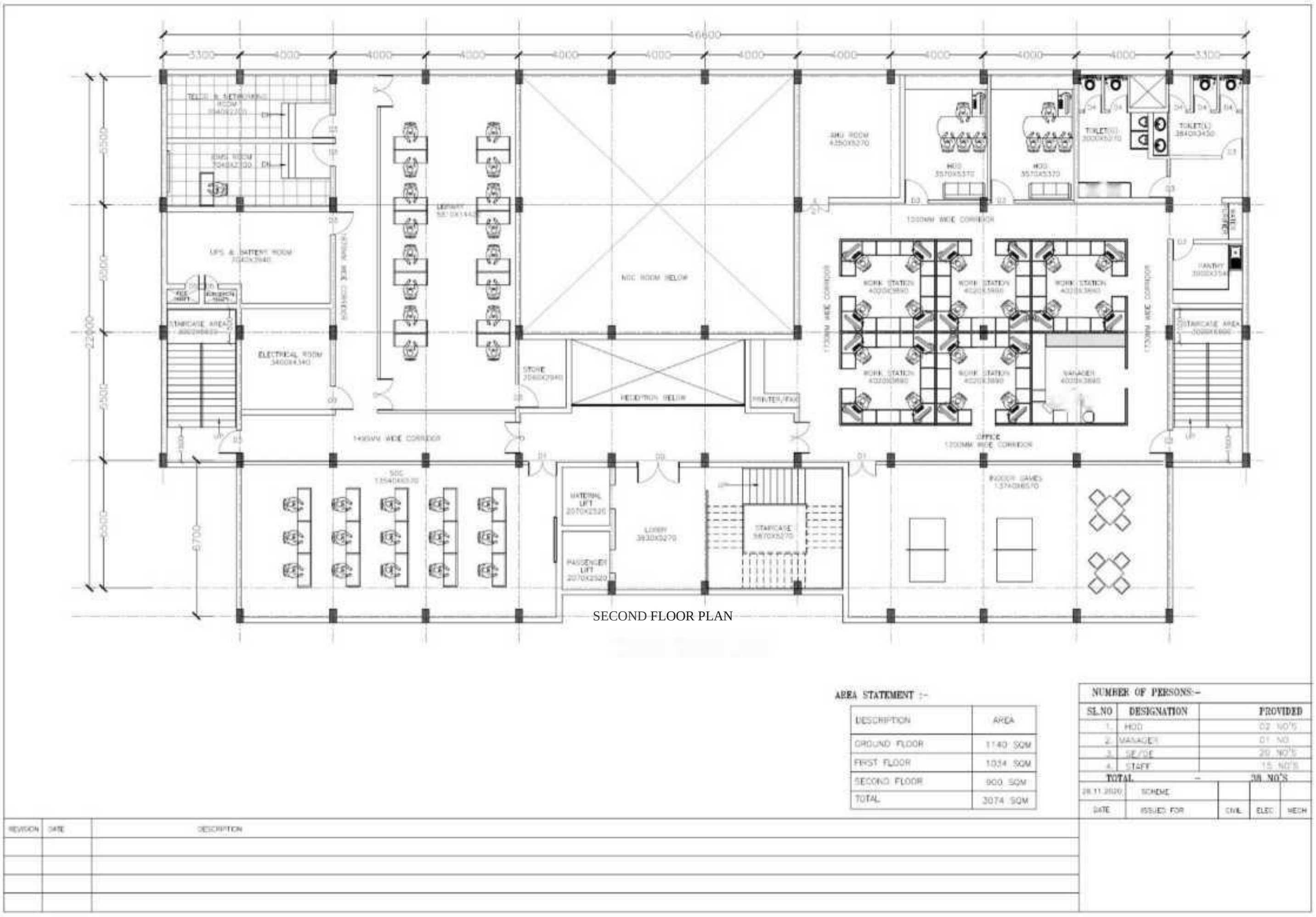
DESCRIPTION	AREA
GROUND FLOOR	1140 SQM
FIRST FLOOR	1034 SQM
SECOND FLOOR	900 SQM
TOTAL	3074 SQM

NUMBER OF PERSONS:-

SL.NO	DESIGNATION	PROVIDED
1.	HOD	03 NO'S
2.	MANAGER	01 NO
3.	SE/DE	20 NO'S
4.	STAFF	50 NO'S
TOTAL	-	74 NO'S

Figure 3-B: Primary DC - Physical Layout (Required)

16. **<u>Suggested DC Layout - Second Floor (The Bidder may submit proposed design for approval).</u>**



AREA STATEMENT :-

DESCRIPTION	AREA
GROUND FLOOR	1140 SQM
FIRST FLOOR	1034 SQM
SECOND FLOOR	900 SQM
TOTAL	3074 SQM

NUMBER OF PERSONS:-

SL.NO	DESIGNATION	PROVIDED
1.	HOD	02 NO'S
2.	MANAGER	01 NO
3.	SE/DE	20 NO'S
4.	STAFF	15 NO'S
TOTAL	-	38 NO'S

28.11.2020	SCHEME			
DATE	ISSUED FOR	CIVIL	ELEC	MECH

Figure 3-C: Primary Data Centre - Physical Layout (Required)

17. **Suggested DC rack layout (The Bidder may submit proposed design for approval).**

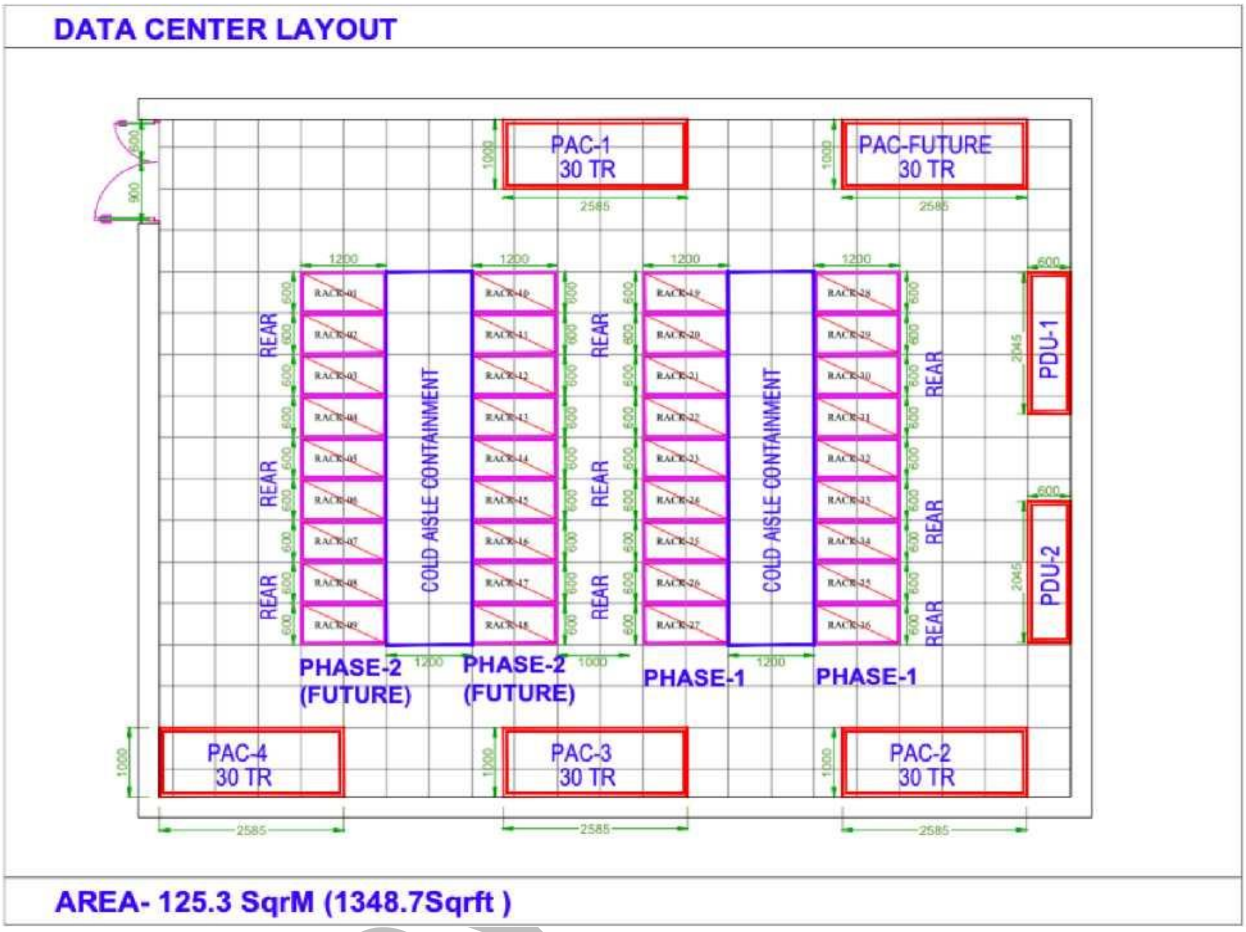
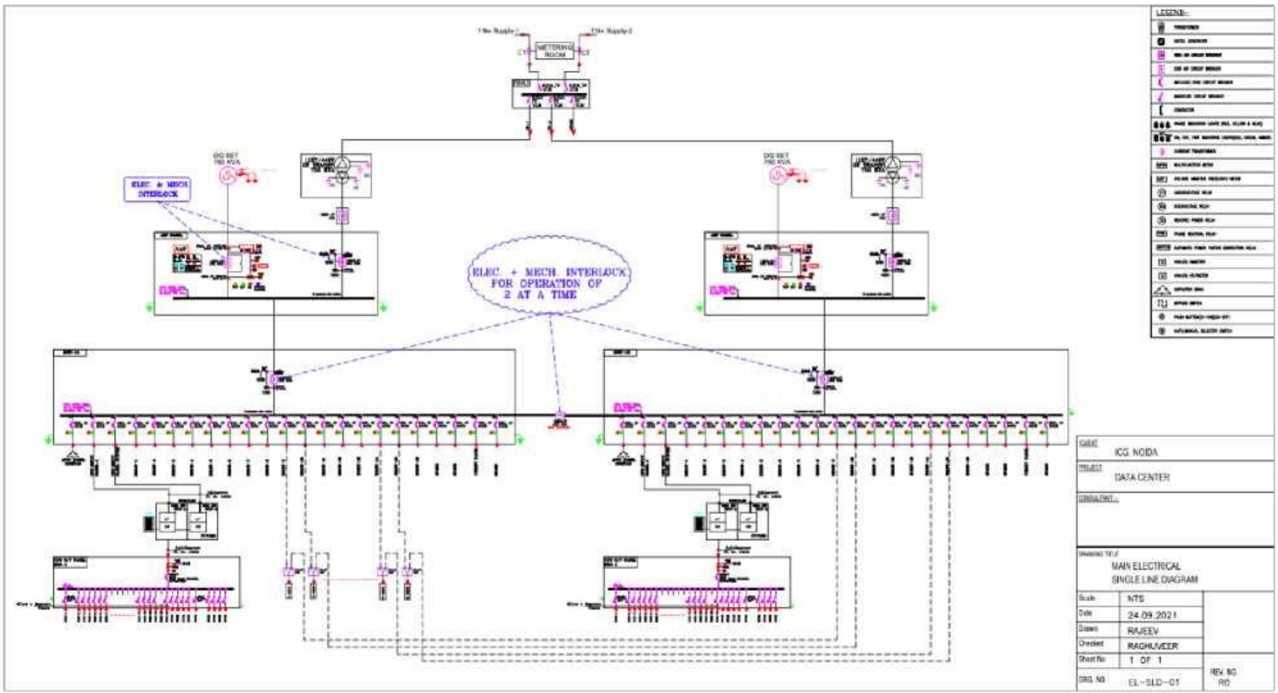


Figure 3-D: Data Centre - Rack Distribution

18. Suggested DC - Power Distribution Layout (The Bidder may submit proposed design for approval).



design for approval).

Figure 3-E: Data Centre - Power distribution Main SLD

VERIFIED

TECHNICAL SPECIFICATIONS: DISASTER RECOVERY DATA CENTRE

Introduction

19. The Disaster Recovery Data Centre (DR-DC) is home to the computational power, storage, and applications necessary to support IT requirements to meet the objectives of Digital Coast Guard which includes Coast Guard administrative, surface/ air, logistics, technical and operational activities, in the event of failure of Main Data Centre. Proper planning of the DR-DC infrastructure design is critical and performance, resiliency and scalability need to be carefully considered.

20. Important aspect of the DR-DC design will be its flexibility to quickly deploy and support new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant advantage. Such a design requires robust initial planning and thoughtful consideration in the area of port density, access layer uplink bandwidth, true server capacity, and oversubscription, to name just a few.

21. Some of the key objectives of the DRC are:-

21.1 Optimal Utilization of space.

21.2 Scalability in phased manner.

Design Objectives.

22 The DR-DC shall be designed catering for following:-

22.1 **Scalability**. DR-DC shall be designed so that capacity be scalable enough for catering to the need of user, data or application growth in future within the same footprint of initial proposal. The quality of the scalability will be judged by the capability of the system to make available the resources in the simplest and quickest manner with minimum or avoiding manual intervention. It is preferred to cater additional equal capacity of IT load scalability option on exhaustion of present designed capacity and required building foundation, structural designing to cater for expansion of further 02 floors in future. Accordingly, additional load-bearing floor equal to present Server & Utility Area may be provisioned and required ground space may earmarked. For better utilisation of additional space, it may be used to cater for non-essential requirements such as car parking, landscape etc. Following scalability requirements will be factored in, but not be limited to, the design criteria of DR- DC:-

22.1.1 Total IT equipment load of 180 Kw.

22.1.2 Phase-I which is present scope, shall cater 90 Kw i.e. about 1/2 of designed capacity.

22.1.3 Future scope, shall cater for additional 90 Kw to achieve full designed capacity of 180 Kw.

22.1.4 DR-DC server room should be able to accommodate a total of 18 Data Racks (10KW each) considering future scalability.

22.1.5 Annualized Power Usage Effectiveness (PUE) of not exceeding 1.5.

22.1.6 DG Set in 1+1 configuration as required and the design of the DR-DC should cater for scalability. Provisioning of DA include installation & commissioning.

22.1.7 Double Conversion Online modular UPS to cater for 90 KW load in Phase-I. Similar capacity need to be added in future. Modular UPS to have 1+1 bank of 100 kW and also each UPS bank to be in N+N configuration to provide adequate high availability.

22.1.8 The cold aisle containment with closed coupled in-row cooling solution should be provided.

22.2 **High Availability**. Availability is best defined as the time the application and the system resources are available to the user on 24x7x365. This is implemented through hardware, software and services. Adequate redundancy at various levels of DR DC is one of the ways of gaining high availability and should be provisioned in order to ensure availability of various applications, database and services. This design objective can be achieved through a modular UPS in N+1 configuration.

22.3 **Interoperability**. The nature of the server room creates an intense need to have access to multiple OS platforms, which aid in application deployments, migrations and updates. Hence, there is a need to accommodate multiple OS platforms within the network, either on one system or multiple systems. Interoperability is an important design parameter, especially for selecting the Storage solution. Storage has to be interoperable with the Servers, HBA, Tape Solution and Backup and Archival Solution.

22.4 **Maintainability**.

22.4.1 Ability to perform routine maintenance without affecting mission critical operations.

22.4.2 Online monitoring of infrastructure system.

22.4.3 Information system with key specifications and operating instructions.

22.5 **Redundancy**.

22.5.1 Modular UPS in N+1 configuration.

22.6 **Security**.

22.6.1 Protection from security breach and man-made threats.

22.6.2 Well defined security policies.

22.6.3 Mix of physical and electronic security measures.

22.7 **Centrally Managed & Monitored Data Centre facility infrastructure & IT infrastructure**. Vendor has to provide **Data Centre infrastructure management (DCIM)** tools to monitor, measure, manage and/ or control data Centre utilization and energy consumption of all IT-related equipment (such as servers, storage and network switches) and facility infrastructure components (such as power distribution units [PDUs] and computer room air conditioners [CRACs]).

23. **Design Sizing**. The clear land will be provided to bidder by ICG. The bidder has to construct the civil infrastructure for approximately 2506 Sq. Mtr (Avg floor area for G+2 with stilt area of 835 Sq Mtr) for DR-DC and similar floor size available for 'Integrated Monitoring & Support Centre'. For that the bidder shall have to involve the Uptime Institute right from design, layout, construction till final handing over of the civil infrastructure. The average power consumption for each server rack to be considered is 10 kW. Layout diagram/ Architectural diagram of the building to be provided by the bidder to ICG within 45 days of signing of contract.

24. **Scope of Work**. The scope of work consists of supply and installation of the following:-

24.1 Bidder has to construct civil infrastructure at ICG provided land for Disaster recovery Centre as per the enclosed layout. Data Centre design should be certified for meeting Tier-III standards by Uptime Institute and relevant certificate to be provided.

24.2 The Complete Electrical Infrastructure from Feeder to the Critical Load including HT, LT with Bus Bar Trunking (BBT) system required to operate and manage the complete DR-DC with respect to equipment and manpower required for this DR-DC.

24.3 The manpower shall be planned for 5 years from the date of acceptance.

24.4 All the equipment supplied should have two years warranty plus 3 years comprehensive AMC cost included in the offered proposal.

24.5 An external boundary/ security wall for approx. 04 acres of land using solid concrete blocks of a height of minimum 2 mtrs with concertina wire rolled over it.

24.6 Racks including high density (10KW) server racks.

24.7 Integrated Data Centre Infrastructure Solution with Prefabricated Full/ Cold/ Hot aisle containment.

24.8 The air-cooled based HVAC solution for the entire building should be offered.

24.9 Software Defined Data Centre (SDDC) enabled Servers, storage and networking devices including virtualization.

24.10 Contained in Row based cooling system.

24.11 Server & Network Racks with IP PDUs.

24.12 VRF or VRV Based HVAC Solution for the DRC complete area.

24.13 Workstations as required.

24.14 Magnetic Whiteboard (1200x2400mm).

24.15 Video Wall for 24x7 monitoring, Super Narrow Bezel LED Display, 24x7 rated, 30′ x 10′ in tile configuration with accessories for "Command Centre" and 20′x10′ for Security Operations Centre (SOC).

24.16 AV Solution for all the meeting & Conference room with VC Capability should be provided.

24.17 Life safety and security systems with following facilities:-

24.17.1 Fire Detection/ alarm & Fire suppression system (Novec 1230 Gas)

24.17.2 Public Address System

24.17.3 VESDA as per uptime tier III certification

24.17.4 Access control with visitor management system

24.17.5 CCTV system

24.17.6 Rodent repellent system

24.17.7 Water leakage detection system

24.17.8 Environmental monitoring system (EMS)

24.17.9 Hydrant Based Fire Fighting System

24.17.10 Integrated Perimeter Security should be provided

24.17.11 Retractable Bollards

24.17.12 Baggage Scanners & Metal Detectors

24.17.13 Under Vehicle Scanners

24.17.14 Office area furnishing (Interiors)

24.17.15 Other Building Services like WTP, STP, Rain Water Harvesting, HSD Yard, DC Building Related Landscaping

25. **Specifications**.

26. **Civil & Interior works**.

26.1 Data recovery Centre civil and interior infrastructure as per the enclosed layout.

26.2 An external boundary/ security wall for approx. 04 acres of land using hollow concrete blocks of a height of 1.5-2 mtrs. With concertina coil on top.

27. **Electrical & UPS works**

27.1 **UPS Specifications**.

27.1.1 UPS to cater Phase-I load i.e. 200 kVA with 10 mins backup with Lithium-ion battery backup suitable to scale up to 400 kVA with N+N configuration to cater Phase-I & Phase-II loads. The UPS should be the latest state-of-the-art modular system and shall be a single unit, complete with modular, parallel redundancy. UPS standards like EN 62040-1:2008, 2011 and 2013 must be followed.

27.1.2 The capacity of the UPS system proposed should take care of server, network, storage and lighting load along with safety margin.

27.1.3 It should be configured in N+N redundancy mode.

27.1.4 The power modules shall be hot-swappable and while the system is running live, removing or replacing power modules shall have no impact on the load. It should be possible to add or replace power modules without switching the load to bypass source. Notification should be provided on the UPS integrated display for add or removal of Power module.

27.1.5 The main system controller shall be hot-swappable and while the system is running live, removing or replacing the main system controller shall have no impact on the load.

27.1.6 The UPS system shall be upwardly scalable by simply adding UPS power modules to the available shelves, and adding more shelves if required with no need of any additional parts.

27.1.7 UPS shall be provided with DCIM interface and integrated with unified IT Operations Management software for centralized monitoring & management.

27.1.8 Battery specification as following:-

27.1.8.1 Lithium-ion of NMC type.

27.1.8.2 Sealed maintenance free batteries.

27.1.8.3 Battery Protection using electronic switch (SCR) & Fuse.

27.1.8.4 Battery housing should be compact and space saving MS steel open racks complete with interconnectors / Battery fuse box or isolator (in case of external protection) - IP 20.

27.1.8.5 Mounted in a rack.

27.1.8.6 The UPS battery shall support replaceable, hot swappable, fused, battery modules.

27.1.8.7 Each battery module shall be monitored for voltage and temperature for use by the UPS battery diagnostic. Battery charging current shall be temperature compensated.

27.1.8.8 The UPS shall incorporate a battery management system to continuously monitor the health of each removable battery module. This system shall notify the user in the event that a failed or weak battery module is found.

27.1.8.9 The Batteries shall be long life batteries (5 years).

27.1.8.10 Battery recharge/ Certification.

27.1.8.10.1 The battery offered shall re-gain its 100% power in 2 hour to 4 hours or less.

27.1.8.10.2 Certification for Li-Ion battery: UN38.3, UL1973.

27.1.8.10.3 Built-in CMU (Cell Management Unit) to monitor individual cell voltage, temperature and manage cell balance.

27.1.8.10.4 Built-in isolated CAN Bus among CMUs & BMU for high voltage battery string operation.

27.1.8.10.5 Operating range for battery without derations in battery capacity - 0°C to 45°C.

27.2 **Electrical Panel and Distribution**. Electrical Panel and Distribution shall consist of minimum of following:-

27.2.1 The Data Recovery Centre main panel will be located in appropriate room and this will distribute the power to the UPS and other utilities.

27.2.2 Required number of PDUs in redundancy.

27.3 **Earthing**. “Maintenance Free Earthing", which uses special highly conductive backfill in place of conventional salt/ charcoal should be provided for all equipment’s protective Earthing. Earthing standards such as IS:3043-1987, IEEE 80:2012 & IEC 62561- 7:2018 must be followed.

27.4 **Lighting and Raw Power Distribution**.

27.4.1 Lighting to be designed for the illumination level of 500 lux at server room and 300 - 350 lux at UPS room.

27.4.2 Light fixtures shall be ceiling/ recess mounted type.

27.4.3 Emergency lighting circuits shall be done to maintain required visibility in case of emergency/main power failure.

27.4.4 Separate DB should be provided which will distribute the power to emergency lighting, Fire and safety security system.

27.4.5 Required number of raw power sockets shall be provided for utility purpose, IT Office area and NOC area.

28. **Cooling Works**.

28.1 Data Centre cooling solution should be in-rack/ in-row based solution to support average density Rack Load of minimum 10KW per rack with 42U useable rack space per rack.

28.2 Data recovery Centre cooling solution should be deployed in phased manner with required Racks, cooling system and other accessories.

28.3 Cooling system should support requirement of 90 KW IT Load in Phase 1 and 90 KW IT Load in second Phase too.

28.4 Cooling Solution should be **DX based.** The remaining of the Data Centre building Cooling should VRV/VRF based Comfort cooling.

28.5 All Electrical and civil work for cooling solution for all phases to be completed in Phase-I. Cooling units will be added as required in the later time for subsequent Phase.

28.6 The Comfort Cooling and the DR-DC Specific Cooling Solution Should be enabled for centralized monitoring using IBMS/ DCIM software.

28.7. **Centralized integrated building air-conditioning**. Entire built-up area of disaster recovery data Centre should be centrally air-conditioned using VRV/ VRF Solution. Should be enabled for centralized monitoring using IBMS software. Should comply fully with latest edition of IS 659:1964 standards.

29. **Fire, Safety & Security Systems**.

29.1 **Access Control System**. It is required to install an electronic access control system that allows only restricted access to different areas based on pre-set access policy. It also logs the entry and exit for auditing later. This system assists in controlling any unauthorized movement within:-

29.1.1 Server Room using card and biometric reader with single person interlock system (to prevent piggy backing).

29.1.2 UPS and Electrical room using card reader

29.1.3 NOC, Telecom room, BMS room using card reader

29.1.4 Generator area and data recovery Centre perimeter area using intrusion detection system.

29.2 **CCTV System**. The primary objective of a CCTV system is to ensure effective 24x7 surveillance of an area and also create a record for post event analysis for 30 days.

29.2.1 Server room, generator area, parking, telecom, NOC, DCIM, BMS and UPS room shall be covered using high resolution, fixed dome camera Closed Circuit Video Surveillance.

29.2.2 Perimeter Security using CCTV.

29.2.3 All camera should be of IP Camera with PoE+ & ONVIF compliance for better integration with other BMS systems.

29.3 **Fire Detection, Alarm system**. The Conventional fire alarm system with multi sensor detector will be connected to the fire alarm control panel through a pair of wires. Manual call points to be provided to trigger the alarms manually in case of emergency situations and also strobes cum hooters are to be provided to give the alarms with sound as well as strobe indications.

29.4 The panels are modular in nature and can be customized to the specific requirement by selecting the suitable housing, rail and modules. The panels are configured based on the requirement

29.5 The conventional fire alarm system to consist of the following systems at different areas of the Data Centre as mentioned below:-

29.5.1 Fire alarm control Panel.

29.5.2 Manual call point.

29.5.3 Strobe cum sounder.

29.5.4 Heat detector for UPS room.

29.6 **Fire suppression system**.

29.6.1 The bidder shall supply, install, test and put in operation NOVEC 1230 based fire suppression system. The fire suppression system shall include and not be limited to gas release control panel, seamless cylinders, discharge valve (with solenoid or pneumatic actuator) as the case may be, discharge pipe, check valve and all other accessories required to make a complete operation system meeting applicable requirements of NFPA 2001 standards and installed in compliance with all applicable requirements of the local codes and standards.

29.6.2 The system design should be based on the specifications contained herein, NFPA 2001 and in accordance with the requirements specified in the design manual of the agent. The bidder shall confirm compliance to the above along with their bid.

29.6.3 Complete Pipe work, Cabling and relevant installation should be catered for entire server room IT infrastructure.

29.6.4 Hand held fire extinguishers shall be provided at NOC/office area and UPS room as follows:-

29.6.4.1 4.5Kg Class CO2 type portable fire extinguishers for UPS Room.

29.6.4.2 ABC Stored Pressure type Fire Extinguisher 6 Kgs. for NOC/ Office/ BMS/generator/ telecom area.

29.7 **Water leak detection and Rodent repellent**.

29.7.1 Tape sensor cables to be provided to detect water leak or flooding. Water leak will cause contact closure in the cable circuit to send an alarm through Panel.

29.7.2 Rodent repellent shall have master control unit with satellite modules which will be located at strategic location and with variable frequency ultrasound to deter the rodents that inhibit the server room.

29.7.3 The Rodent Control System should withstand high temperature fluctuations and should not cause any sparking.

29.8 **Environmental Monitoring System**. Environmental Monitoring system should be able to monitor the Temperature, humidity and leak in the server room and UPS room environment.

29.8.1 It should be capable to measure temperature and humidity in each rack.

29.8.2 IP based and be able to monitor from remote locations.

29.8.3 It should be capable to integrate with building management system.

29.8.4 It should be rack mountable type

29.9 **BMS and NMS Systems**.

29.9.1 The Building Management System will be implemented to monitor the various systems installed later. Entire server room should be monitored with the DCIM System (BMS) and Network Management System (NMS). All Data Recovery Centre components should be provided with suitable BMS/ NMS interface modules. All required cables and relevant accessories to be laid.

29.9.2 IP enabled PDU compatible to BMS with the following design:

29.9.2.1 Sleek design

29.9.2.2 Locking power chord.

29.9.2.3 Temperature/ humidity sensor compatibility

29.9.2.4 Ability to generate threshold value to generate e-mail alert

29.9.2.5 Ability to generate data reports of temperature/ humidity/ ampere/ kw/ kwh.

29.9.3 BMS will be capable of monitoring each cooling system, UPS, Electrical Panels and complete security system such as Fire alarm system, fire suppression system, EMS, ACS, VESDA, WLD, etc.

30. **Software Defined Data Centre (SDDC) enabled Server, Server Chassis, Software, Main Storage and Backup Tape Storage Systems**. Detailed minimum sizing and IT infrastructure technical specifications are given in Chapter-06 of this DPR.

31. **Installation and Support**. Installation support for all related software, hardware, networking, storage configuration including Windows 2016 Active Directory, Virtualization, Backup and User/Administrator setup.

32. **Fuel System**. Design architecture of fuel system must be in accordance with Tier-III data centre standards. The path of fuel supply and return lines must be either concurrently maintainable or fault tolerant. The fuel system components namely pumps, manual valves, automated valves, control panels and tanks must meet either the concurrently maintainable or fault tolerant objective. All piping inclusive of fittings and valves shall follow the applicable BIS codes. Specification of pipe, pie fittings and valves are enumerated below:-

32.1 Pipes shall be MS class 'C'& fittings shall be welded type fittings conforming to relevant BIS codes. All jointing in the pipe system shall generally be by welding/ flanges unless otherwise mentioned or directed at site.

32.2 All pipes and their steel supports shall be thoroughly cleaned and given on primary coat of red oxide paint before being installed. All welded piping shall be subject to the approval at site.

32.3 Thread joint fittings shall be malleable casting of pressure rating suitable for the piping system.

32.4 Tee-off connections shall be through equal or reducing tees other-wise ferrules welded to the main pipe shall be used.

32.5 Flanges shall be approved make. The supply of flanges shall also include supply of bolts and nuts and suitable asbestos fibre/ rubber insertion gaskets (minimum 3 mm thick).

32.6 Swing check valves shall normally be used in all services. Lifts type valves may be used in horizontal runs.

32.7 The strainers shall be of cast iron body with gunmetal or bronze mesh for fine filtration of the oil.

32.8 All piping and fitting shall be pressure tested, then painted and shall be provided with additional weather proof treatment for buried pipes.

32.9 Supply of diesel to day oil tank from the bulk oil storage tank shall be automatically controlled by providing level sensor on each tank and controlled by Solenoid valves. Single pipe line shall feed to number of tanks.

32.10 System shall be provided to return the diesel fuel automatically back to the bulk storage tank in the case of pump supplying diesel from the bulk storage tank to the day oil tank over runs. Pump capacity and Head shall be worked out by the vendor on the basis of Site condition.

33. **Miscellaneous**.

33.1 **Glow Signage**. Glow signage on both sides of the door shutters marking PUSH / PULL along with other signage marking for different work areas and emergency signs.

33.2 **Shoe Rack**. At entry of Server Room to avoid entry of dust in server room.

33.3 **Name plate**. Suitable aesthetically designed brass name plate containing “Data Recovery Data Centre" to be affixed in the entrance.

33.4 **Work stations**. 120 work stations of data centre specification to be provisioned in DR. Cabin to cubicle ration is 20:80. Size of the cabin - 10'x15' and cubicles - 8'x6'. Each cabin/ cubicle to be equipped with one Desktop computer(minimum i7 or equivalent processor, RAM- DDR4 8 GB & Storage 1TB, 22” LED Monitor, 1 KVA UPS). DR to be provided with 04 Heavy Duty MFDs and 15 printers each (05 color and 10 BW).

33.5 **Work space amenities**. DR to be provisioned with Common area, Conference Rooms, Terrace Open Area, Store Rooms, wet canteen, Dining Space, Restrooms, Lobby and Lounge with adequate furniture.

33.6 **Parking space**. Parking space should be able to accommodate 50 four wheelers and 60 two wheelers.

33.7 **Industrial RO plant and portable water dispensers**. DR to be equipped with one industrial RO plant (Minimum 250 Ltr/ Hour capacity). Two heavy duty water dispensers to be provisioned in each floor with direct connectivity from RO plant.

33.8 **Lightening Aarresters**. Lightening protection system complying with recognized safety standards of LPI175, NFPA780 and UL96A to be installed in the data Centre to avoid downtime, outage and service interruption caused by the after effect of Lighting.

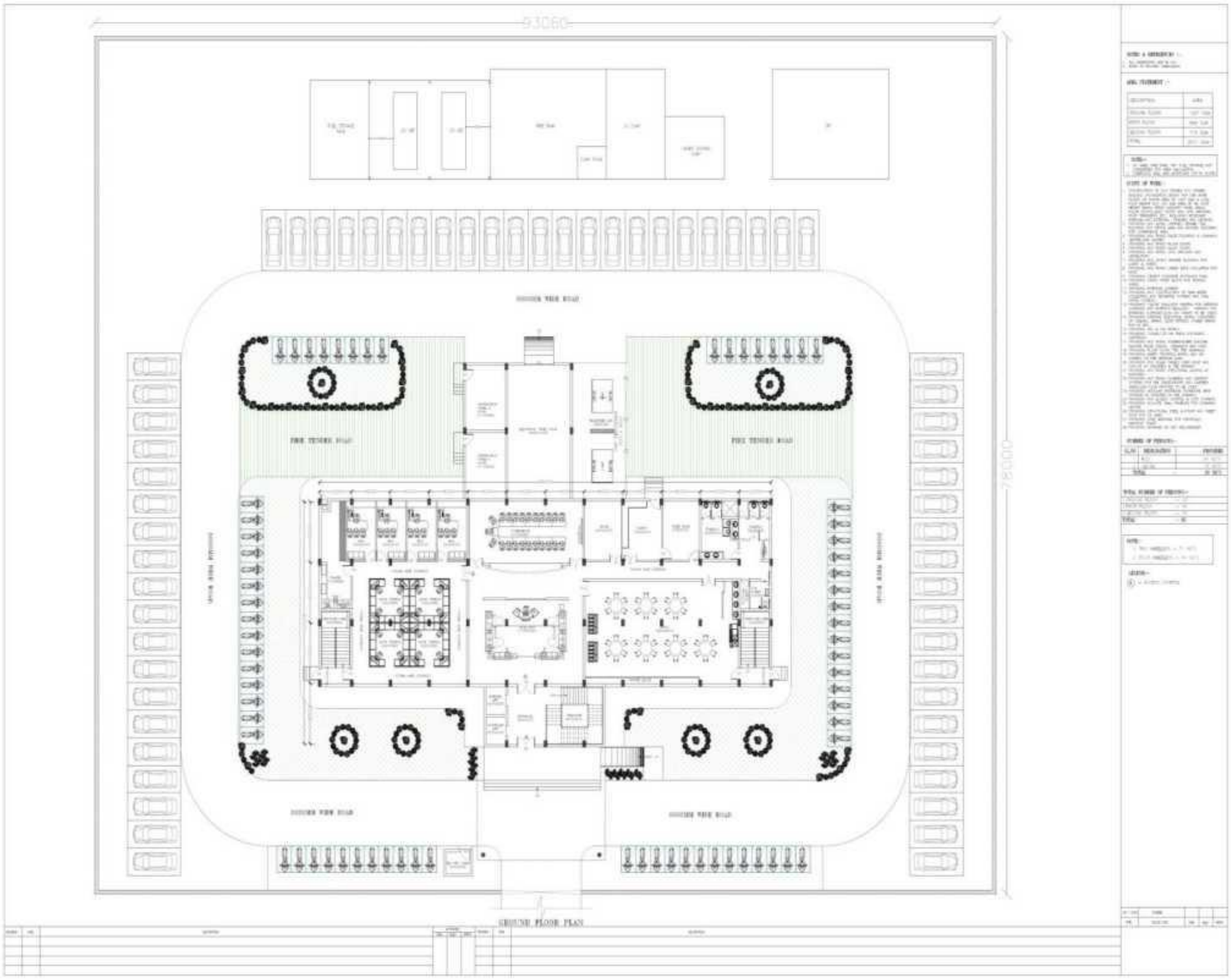
34. **Data Recovery Data Centre-High level Bill of Material**

Sl.	Item	Qty	UOM
34.1	DR DC Civil, Electrical and Interiors	1	Set
34.2	DR DC In-Row Cooling Solution	1	Set
34.3	Centralised Integrated Building Air conditioning using VRV/VRF system	1	Set
34.4	Modular UPS 200 KVA scalable to 400 KVA for server room	1	No.
34.5	Fire Alarm & Novec 1230 based Gas Suppression System	1	Set
34.6	Rodent Control System	1	Set
34.7	Water Leak Detection System	1	Set
34.8	DCIM Software	1	No.
34.9	Environment Management System (EMS)	1	No.
34.10	Biometric Door Access System (as required)	1	Set
34.11	IP Dome Surveillance Camera (as required)	1	Set
34.12	Portable Fire Extinguisher (as required)	1	Set
34.13	DG Set 150KVA with AMF	1	Set
34.14	Server Racks of 10 KW capacity	18	No.
34.15	Transformer, HT panel and PCC	1	Set
34.16	IT infrastructure as per detailed technical specifications	1	Set
34.17	Video Wall for 24x7 monitoring, Super Narrow Bezel LED Display, 24x7 rated, Full-HD, 700nit, HTML5 browser, 30’x10’ in tile configuration with accessories for “Command Centre” and “20’x10‘ for Security Operations Centre (SOC)	1	Set
34.18	Media Safe	1	No.

34.19	Command and Control Centre Software System (as required)	1	Set
34.20	Workstations one Desktop computer (minimum i7 or equivalent processor, RAM- DDR4 8 GB & Storage 1TB)	120	Nos.
34.21	Structured Cabling	1	Set
34.22	KVM Switch with Console	1	Set
34.23	Antivirus Software solution	1	Set
34.24	External boundary/ security wall for 04 acres of land	1	Set

35. **Suggested Disaster Recovery Data Centre Layout (The Bidder may submit proposed design for approval).**

35.1 **DR-DC - Ground Floor**



VERIFIED

35.2. **DR-DC - First Floor**

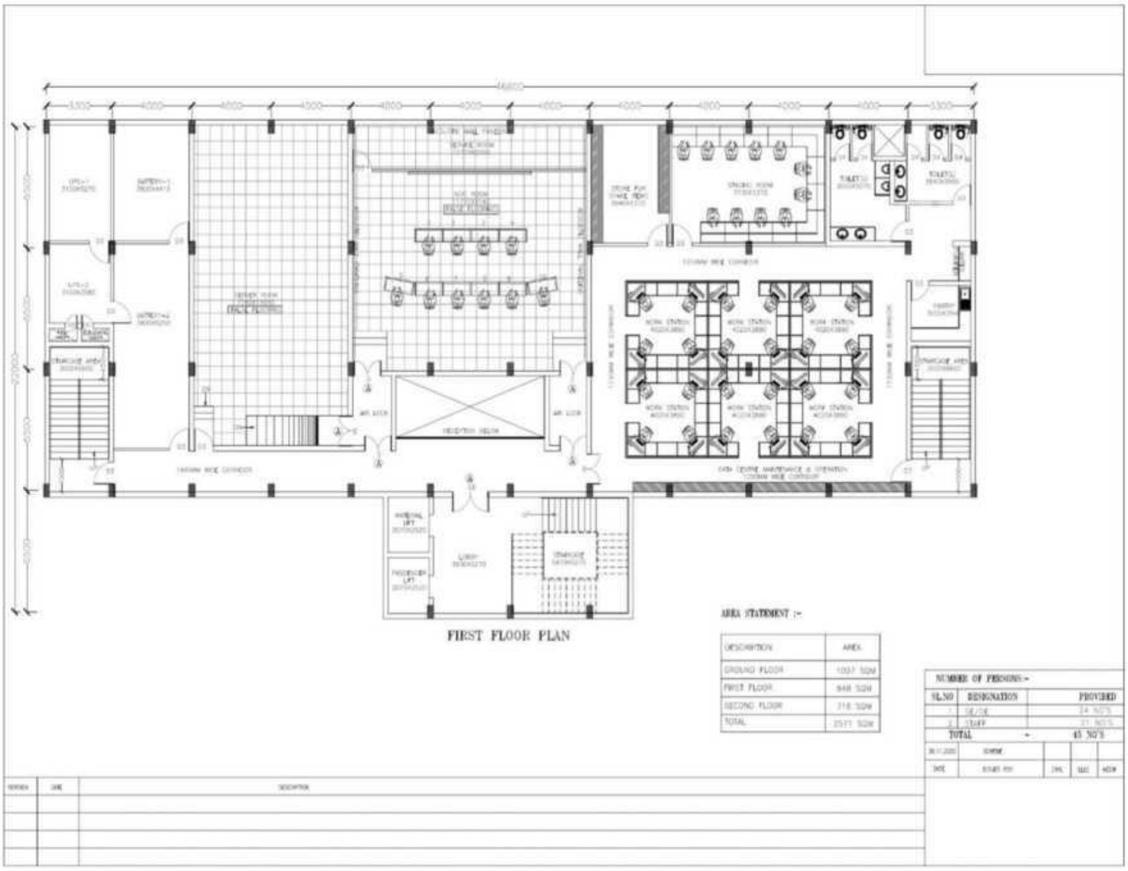
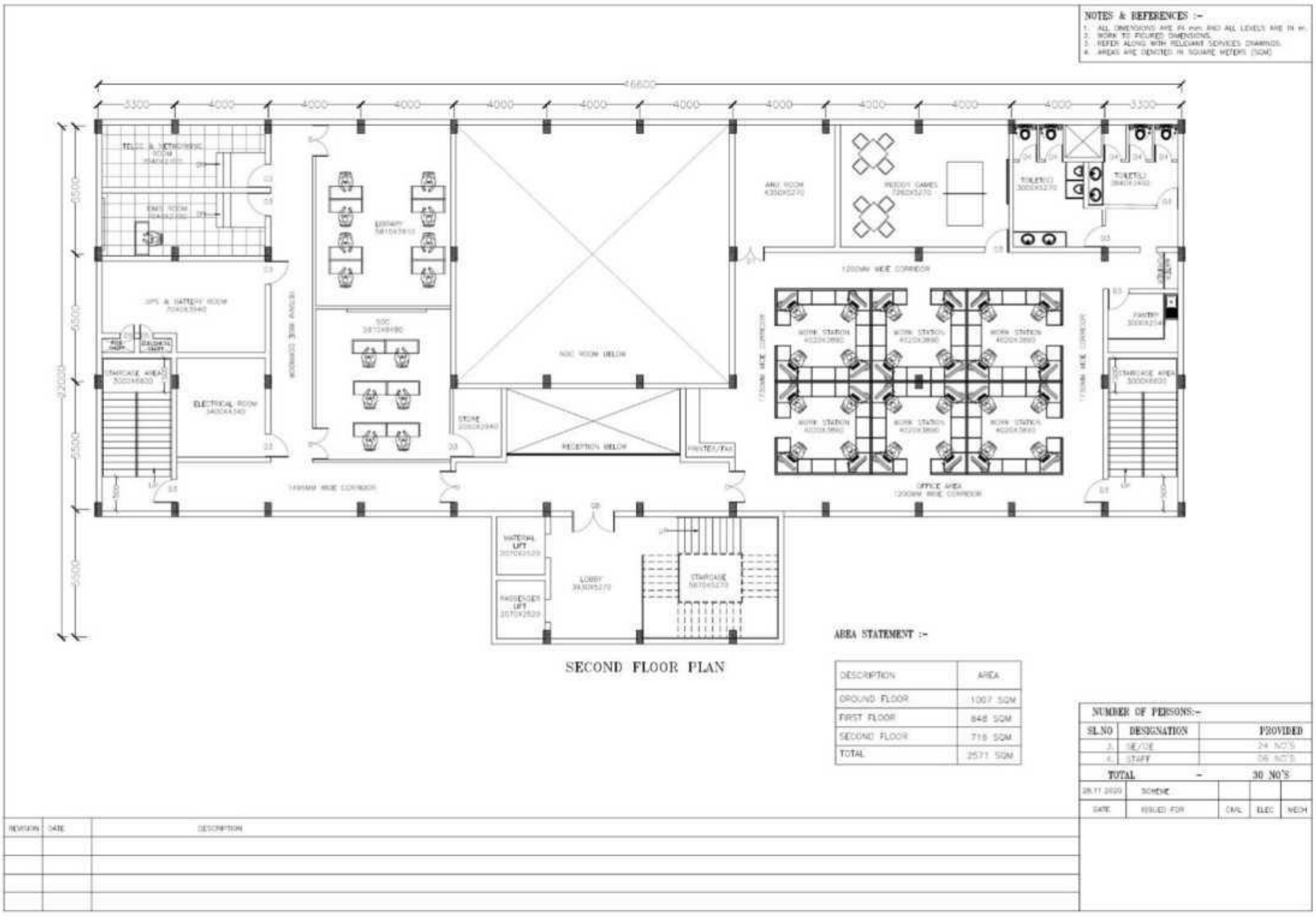


Figure 3-B: Disaster Recovery Data Centre - Physical Layout (Required)

35.3. **DR-DC - Second Floor**



SECOND FLOOR PLAN

NOTES & REFERENCES :-

1. ALL DIMENSIONS ARE IN mm AND ALL LEVELS ARE IN m.
2. WORK TO FIGURED DIMENSIONS.
3. REFER ALONG WITH RELEVANT SERVICES DRAWINGS.
4. AREAS ARE DENOTED IN SQUARE METERS (SQM)

AREA STATEMENT :-

DESCRIPTION	AREA
GROUND FLOOR	1007 SQM
FIRST FLOOR	848 SQM
SECOND FLOOR	716 SQM
TOTAL	2571 SQM

NUMBER OF PERSONS:-

SL.NO	DESIGNATION	PROVIDED
3.	SE/OE	24 NO'S
4.	STAFF	06 NO'S
TOTAL	-	30 NO'S

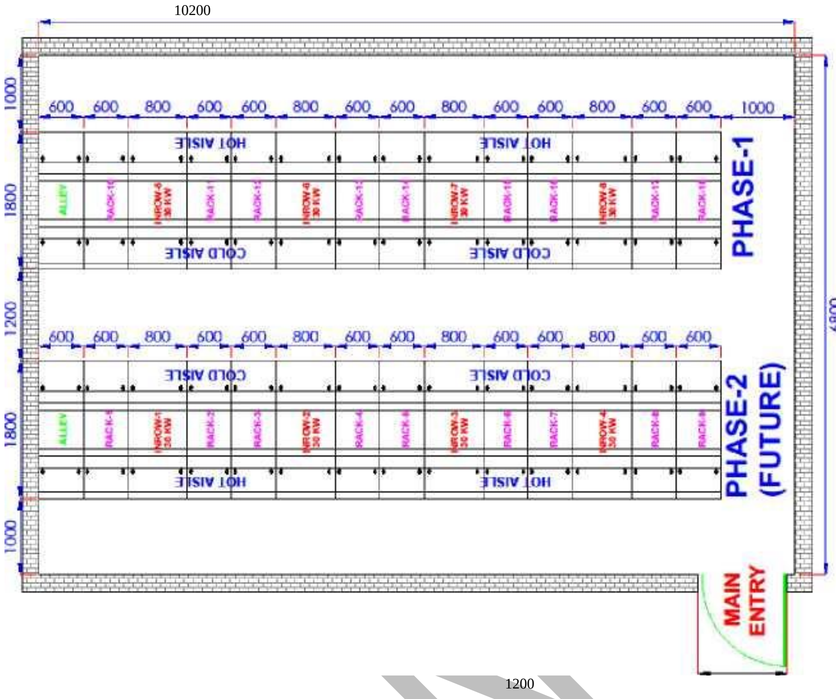
28.11.2020	SCHEME			
DATE	ISSUED FOR	CIVIL	ELEC	MECH

REVISION	DATE	DESCRIPTION

VERIFIED

35.4 DR-DC - Rack Layout

DISASTER RECOVERY DATA CENTRE LAYOUT



AREA- 69.4 SqrM (747.1 Sqrft)

Figure 3-D: Disaster Recovery Data Centre - Physical Layout (Required)

VERIFIED

35.5 **DR-DC Power Distribution Layout**

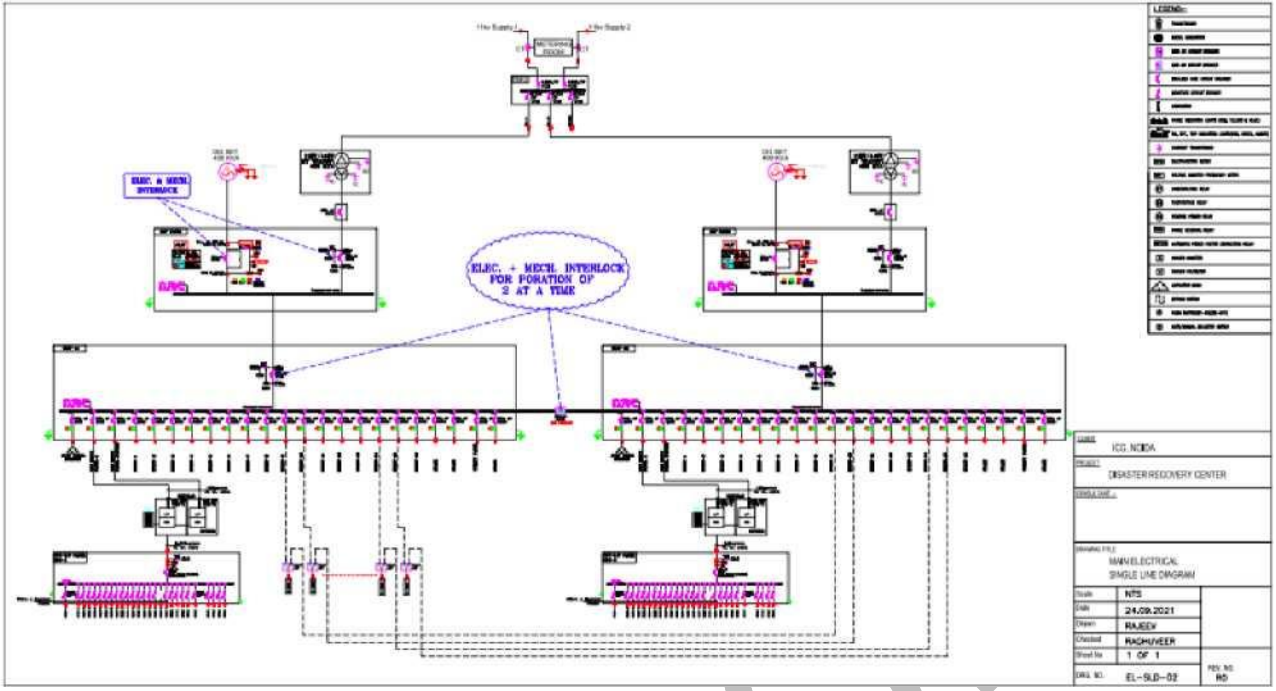


Figure 3-E: Disaster Recovery Centre - Power distribution Main SLD

TECHNICAL SPECIFICATIONS: NEAR LINE DATA CENTRE

Introduction

36. Applications running at Data centre are mostly business critical and support multiple essential functions of the organizations, e.g., HR, Finance, inventory management, logistics, planning, reporting, security, governance & compliances etc. It is thus imperative to set up a sound business continuity and disaster recovery policy, so that such business applications can be made available within shortest possible time from alternate location. Disaster Recovery Data canter (DR) is set up by the organizations to meet these needs. Data at main DC is replicated at DR setup, which is based on organization's RTO/RPO requirements (RTO being the time organization can sustain for the application(s) to come up again from DR site, and RPO is the amount of data loss acceptable to the organization). DR Centre is brought up in case of any disaster to serve the users within defined RTO/RPO requirements.

37. As per best practices, the DR data centres are created in far locations, mostly in different seismic zones to meet applicable guidelines. More often, other factors also kept in mind while selecting DR Centres to compensate for any frequent natural incidents (e.g., if DC at flood prone area, DR is setup at a comparatively higher altitude). While this approach meets the guideline requirements and prepares the organization for any untoward disaster/ natural calamity, the distance between the locations has direct impact on data replication capabilities- the more the distance, the more time it takes to travel the data between. Also, the cost of bandwidth increases significantly with the distance. This results in low bandwidth, high latency replication link between DC and DR, forcing asynchronous replication of data, hance higher RTO/ RPO (usually in the range of 2-4 hours).

38. In DCG project, Uptime Tier -III certification is envisaged that requires 99.98% of uptime of services. For achieving very low or near-zero RTO/ RPO (i.e., near immediate availability of applications without any major data loss, in case of disaster), a third data Centre setup, generally called as "Near Line DC/ DR (NLDC/ NDR) "is required near the main DC, within permissible direct connectivity limits for synchronous replication (direct fiber connectivity supported up to 50-70 Km).

39. In this Data Centre arrangement, all/ critical applications' data will be replicated synchronously between main DC and NLDC, while replication between main DC and far DR will continue asynchronously. Depending on the situation BC/ DR policy, in case of any failure/ disaster at DC, such applications can either be instantaneously brought up from NLDC location without any significant lag and without any major data loss, or the far DR can be brought up for all applications with delta replication of remaining data from NLDC site. Depending upon applications, databases and infrastructure capabilities,

customers can achieve near zero RTO/RPO in a Data Centre setup. Data Centre setup is necessity for ICG to achieve the purpose of serving large number of internal/ external users across a large geography with business applications.

Design requirement

40. Only the **clear land** will be provided by Coast Guard to the SI for construction of Near Line Data Centre (NLDC). The SI has to establish the NLDC as per standard. The NLDC Shall be made within the same campus as of the DC. The NLDC shall be designed catering for following:-

40.1 Total IT equipment load of 50 Kw (5 Racks of 10 Kw Each).

40.2 DG Set of 100KVA in N+N configuration as required. Provisioning of DA includes installation and commissioning.

40.3 Double Conversion Online modular UPS system of 60KW in N+N configuration should be provided for the NLDC. Batteries of Lithium-ion type be provided to support a backup time of 10 minutes.

40.4 The cold aisle containment with perimeter cooling solution should be provided.

40.5 LT panel of 100 KVA in N+N configuration.

40.6 The NLDC shall be provided as a Hot & Cold aisle containment Smart Row solution with 5 Racks Having 3 In-Row units of the capacity mentioned above. The UPS can be placed in electrical room specifically designed for the NLDC.

40.7 **High Availability**. Availability is best defined as the time an application and the system resources are available to the user on 24x7x365. This is implemented through hardware, software and services. Adequate redundancy at various levels of DC is one of the ways of gaining high availability and should be provisioned in order to ensure availability various applications, database and services.

40.8 **Maintainability**. Ability to perform routine maintenance without affecting mission critical operations

40.9 **Redundancy**.

40.9.1 Considerations on secondary components becomes vital in the event of a primary component failure.

40.9.2 Elimination of single points of failure wherever feasible.

40.9.3 Redundancy of N+1 for Cooling system, N+N for UPS, Dual-Feed of raw power supply circuits etc.

40.10 **Security**.

40.10.1 Protection from security breach and man-made threats.

40.10.2 Well defined security policies.

40.10.3 Mix of physical and electronic security measures.

40.11 **Centrally managed & monitored data centre facility infrastructure & IT infrastructure.** Vendor to provide Data Centre Infrastructure Management (DCIM) tools monitor, measure, manage and/or control data centre utilization and energy consumption of all IT-related equipment (such as servers, storage and network switches) and facility infrastructure components (such as power distribution units [PDUs] and computer room air conditioners [CRACs]).

40.12 **Design Sizing**. Civil infrastructure of approximately 50 Sq. mtr are to be constructed for NLDC. For that the bidder shall have to involve the Uptime Institute right from design, layout, construction till final handing over of the civil infrastructure. The average power consumption for each server rack to be considered is 10 kW. The bidder has to provide layout diagram/ architectural diagram of the NLDC within 45 days of signing the contract.

41 **Scope of Work**. The scope of work for NLDC consists of supply and installation of the following:-

41.1 Bidder to construct NLDC civil and interior infrastructure as per the Designated Area Size.

41.2 The Complete Electrical Infrastructure from Feeder to the Critical Load including LT with BBT required to operate and manage the complete NLDC with respect to equipment required for this NLDC.

41.3 High density server racks be provided.

41.4 Software Defined Data Centre (SDDC) enabled servers, storage and networking devices including virtualization, clustering, etc.

41.5 Closed coupled in-row cooling with hot and cold aisle containment.

41.6 Life safety and security systems with following facilities:-

41.6.1 Fire Detection/alarm & Fire suppression system (Novec 1230 Gas)

41.6.2 Access control with visitor management system

41.6.3 CCTV system

41.6.4 Rodent repellent system

41.6.5 Water leakage detection system

41.6.6 Environmental monitoring system (EMS)

41.6.7 Integrated Perimeter Security should be provided

42 **Specification**

42.1 **Civil & Interior works**. NLDC civil infrastructure as per the enclosed layout. The outer elevation and colour of the building should be designed in consultation with ICG.

42.2 **Finish**. Top covering with high pressure antistatic hot-pressed laminate 1.00mm thick, factory finish in universal white colour and grey streamlet pattern. Edge bonded with black conductive PVC beading.

42.3 **Tile**. All steel construction & cavity filled with epoxy mix cement. Top plate 0.70, Bottom plate 0.70mm of steel with grey colour powder coated on a continuous line having 64 round embossing to the bottom plate with 100 spot welding to weld top & bottom plate.

42.4 **Pedestal**. All steel constructions & yellow Zinc plated 25mm Dai pipe pedestal with bottom plate of 100mm x 100mm x 2mm thick. Top plate of 75mm x 75mm x 3mm thick with threaded bolt & 2 nuts for levelling adjustment.

42.5 **Stringer**. Stringers of 0.80 mm thick rectangular pipe of size - 20mm (W) x 30mm (Ht.) x 573 mm long, 2 holes centre to centre 550 mm. Special feature of the Product:

42.5.1 Factory finish laminates.

42.5.2 Conductive edge beading.

42.5.3 Solid concrete field, higher load bearing capacity.

42.5.4 Special weather coating on back surface of the tiles.

42.5.5 Totally fire proof.

42.5.6 Fast & accurate installation.

42.6 **Mode of measurement**. Any cut plate up to 300mm width will be charged as 300mm width for measurement & cut plate above 300mm width will be charged as full plate (600mm). No deduction shall be given for any opening & cutouts.

42.7 **Fire Rated Door**

42.7.1 Door leaf Single/Double shall be 46mm thick fully flush double skin door with vision panel of 300 x 300 mm size fitted with fire rated glass. Door leaf shall be manufactured from 1.6 mm minimum thick galvanized steel sheet Fe 355 grade (not re-rolled). The internal construction of the door should be rigid reinforcement pads for receiving appropriate hardware. The infill material shall be resin bonded honeycomb core. Fully flush, double skin door shell with lock seam joints at stile edges. Internal reinforcements shall be provided at top, bottom & stile edges for fire rating.

42.7.2 Hinges are to be provided of SS 316 grade Stainless steel double ball bearing butt hinges of size 100mm x 76mm x 3mm thick conforming to BS 7352 standard for 'Strength and durability performance of metal hinges for side hanging applications and dimensional requirements for template drilled hinges' and are classified in class 8 ie, with 20000 annual operations. The screws for hinges shall be SS 316 grade Philips head CSK screws of size M6x 15mm.

42.7.3 All fire doors must be hung on minimum four no steel hinges, to resist bowing in the event of a fire and to bear the increased weight of the door.

42.7.4 Fire resisting doors must be fitted with external dual action hydraulic type self-closing devices which are adjusted to close quickly but latch slowly so as not to wear the smoke seals or damage the door or frame. Perco-type closers are not suitable as they cause the doors to slam causing noise nuisance to occupiers and they tend to wear the smoke seals/frames causing damage over a period of time. Self-closers are to be attached using appropriate fixings ("snake eye screws") which are designed to prevent removal/ tampering by user.

42.7.5 All doors and frames shall be suitably cleaned and primed with two component epoxy primer and finished with polyurethane aliphatic grade paint of approved color. The door leaf and frame shall have passed minimum 500 hours of salt spray test.

42.7.6 Door Accessories shall be similar fire rating as of Doors.

42.7.7 The fire Doors with frame shall be as per IS: 3614 part 4 and BS: 476 part 20, and tested at FRL CBRI Roorkee or ARAI with standard heating conditions as specified in IS: 3809 - 1979 and BS: 476 part 20 & 22 1987 all complete to the entire specification with the certified copy of the valid Test Certificates to be issued by OEM.

43. **Electrical & UPS works**.

43.1. **UPS Specifications**.

43.1.1 60 KW modular UPS in N+N configuration and Lithium-ion Battery banks to provide minimum 10 minutes back up at full load. Should be integrated with DCiM software for centralized monitoring & management.

43.1.2 The UPS should be the latest state-of-the-art modular system and shall be a single unit, complete with modular, parallel redundancy with Lithium-ion batteries. UPS standards like EN 62040-1:2008, 2011 and 2013 must be followed.

43.1.3 The capacity of the UPS system proposed should take care of server, network, storage and lighting load along with safety margin.

43.1.4 It should be configured in N+N redundancy mode.

43.1.5 The power modules shall be hot-swappable and while the system is running live, removing or replacing power modules shall have no impact on the load. It should be possible to add or replace power modules without switching the load to bypass source. Notification should be provided on the UPS integrated display for add or removal of Power module.

43.1.6 The main system controller shall be hot-swappable and while the system is running live, removing or replacing the main system controller shall have no impact on the load.

43.1.7 The UPS system shall be upwardly scalable by simply adding UPS power modules to the available shelves, and adding more shelves if required with no need of any additional parts.

43.1.8 UPS shall be provided with BMS interface and integrated with unified IT Operations Management software for centralized management & monitoring.

43.2 **Battery specification as following**

43.2.1 Lithium-ion of NMC type.

43.2.2 Sealed maintenance free batteries.

43.2.3 Battery Protection using Electronic switch (SCR) & Fuse.

43.2.4 Battery housing should be compact and space saving MS steel open racks complete with interconnectors/ Battery fuse box or isolator (in case of external protection) - IP 20.

43.2.5 Mounted in a rack.

43.2.6 The UPS battery shall support replaceable, hot swappable, fused, battery modules.

43.2.7 Each battery module shall be monitored for voltage and temperature for use by the UPS battery diagnostic. Battery charging current shall be temperature compensated.

43.2.8 The UPS shall incorporate a battery management system to continuously monitor the health of each removable battery module. This system shall notify the user in the event that a failed or weak battery module is found.

43.2.9 The Batteries shall be long life batteries (5 years).

43.2.10 Battery recharge/ Certification:-

43.2.11 The battery offered shall re-gain its 100% power in 2 hour to 4 hours or less.

43.2.12 Certification for Li-Ion battery: UN38.3, UL1973

43.2.13 Built-in CMU (Cell Management Unit) to monitor individual cell voltage, temperature and manage cell balance.

43.2.14 Built-in isolated CAN Bus among CMUs & BMU for high voltage battery string operation.

43.2.15 Operating range for battery without deration in battery capacity - 0 to 45 deg C

43.3 **Electrical Panel and Distribution**. ElectricalPanel and Distribution shall consist of minimum of following:-

43.3.1 The Data Centre main panel will be located in appropriate room and this will distribute the power to the UPS and other utilities.

43.3.2 Required number of PDUs in redundancy.

43.4 **Earthing**. "Maintenance Free Earthing", which uses special highly conductive backfill in place of conventional salt/ charcoal should be provided for all equipment's protective earthing. Earthing standards such as IS:3043-1987, IEEE 80:2012 & IEC 62561- 7:2018 must be followed.

43.5 **Lighting and Raw power distribution**

43.5.1 Lighting to be designed for the illumination level of 500 lux at server room and 300 - 350 lux at UPS room.

43.5.2 Light fixtures shall be ceiling/ recess mounted type

43.5.3 Emergency lighting circuits shall be done to maintain required visibility in case of emergency/main power failure.

43.5.4 Separate DB should be provided which will distribute the power to emergency lighting, Fire and safety security system.

43.5.5 Required number of raw power sockets shall be provided for utility purpose, IT Office area and NOC area.

44. **Cooling works**. Closed coupled in-row cooling with hot and cold aisle containment. Suitable Monitoring software to be provided for monitoring the complete health of the cooling solution.

45. **Fire, Safety & Security Systems**

45.1. **Access control system**. It is required to install an electronic access control system that allows only restricted access to different areas based on pre-set access policy. It also logs the entry and exit for auditing later. This system assists in controlling any unauthorized movement within:-

45.1.1. Server Room using card and biometric reader with single person interlock system (to prevent piggy backing).

45.1.2. UPS and Electrical room using card reader.

45.2. **CCTV system**. The primary objective of a CCTV system is to ensure effective 24x7 surveillance of an area and also create a record for post event analysis for 30 days.

45.2.1. Server room, BMS and UPS room shall be covered using high resolution, fixed dome camera Closed Circuit Video Surveillance.

45.2.2. Perimeter Security using CCTV.

45.2.3. All CCTV cameras should be IP, PoE enabled and comply to ONVIF standards.

45.3. **Fire Detection, Alarm System**. The Conventional fire alarm system with multi sensor detector will be connected to the fire alarm control panel through a pair of wires. Manual call points to be provided to trigger the alarms manually in case of emergency situations and also strobes cum hooters are to be provided to give the alarms with sound as well as strobe indications. The panels are modular in nature and can be customized to the specific requirement by selecting the suitable housing, rail and modules. The panels are configured based on the requirement. The conventional fire alarm system to consist of the following systems at different areas of the Data Centre as mentioned below:-

45.3.1. Fire alarm control Panel

45.3.2. Manual call point

45.3.3. Strobe cum sounder

45.3.4. Heat detector for UPS room

45.4. **Fire Suppression System**

45.4.1. The bidder shall supply, install, test and put in operation NOVEC 1230 based fire suppression system. The fire suppression system shall include and not be limited to gas release control panel, seamless cylinders, discharge valve (with solenoid or pneumatic actuator) as the case may be, discharge pipe, check valve and all other accessories required to make a complete operation system meeting applicable requirements of NFPA 2001 standards and installed in compliance with all applicable requirements of the local codes and standards.

45.4.2. The system design should be based on the specifications contained herein, NFPA 2001 and in accordance with the requirements specified in the design manual of the agent. The bidder shall confirm compliance to the above along with their bid.

45.4.3. Complete Pipe work, cabling and relevant installation should be catered for entire server room IT infrastructure.

45.4.4. 4.5Kg Clean Agent ABC type portable fire extinguishers to be provided for UPS Room.

46. **Water Leak Detection and Rodent Repellent**

46.1. Tape sensor cables to be provided to detect water leak or flooding. Water leak will cause contact closure in the cable circuit to send an alarm through Panel locally and through BMS to concerned.

46.2. Rodent repellent shall have master control unit with satellite modules on at least 6 variable frequencies to change alternatively which will be located at strategic location and with variable frequency ultrasound to deter the rodents that inhibit the server room.

46.3. The Rodent Control System should withstand high temperature fluctuations and should not cause any sparking.

47. **Environmental Monitoring System**. Environmental Monitoring system should be able to monitor the Temperature, humidity in the server room and UPS room environment.

47.1. It should be capable to measure temperature and humidity in each rack.

47.2. IP based and be able to monitor from remote through BMS.

47.3. It should be capable to integrate with building management system.

47.4. It should be rack mountable type.

47.5. IP enabled PDU compatible to BMS with the following design:-

47.5.1. Sleek design.

47.5.2. Locking power chord.

47.5.3. Temperature/ humidity sensor compatibility.

47.5.4. Ability to generate threshold value to generate e-mail alert.

47.5.5. Ability to generate data reports of temperature/ humidity/ ampere/ kw/ kwh.

47.6. BMS will be capable of monitoring each cooling system, UPS, Electrical Panels and complete security system such as Fire alarm system, fire suppression system, EMS,

48. **Miscellaneous**

48.1. **Glow Signage**. Glow signage on both sides of the door shutters marking PUSH/ PULL along with other signage marking for different work areas and emergency signs.

48.2. **Name Plate**. Suitable aesthetically designed brass name plate containing "Data Centre" to be affixed in the entrance, Electrical room, First Aid Box, Shock treatment chart, Emergency Rescue Instruction chart and insulated gloves for Electricians.

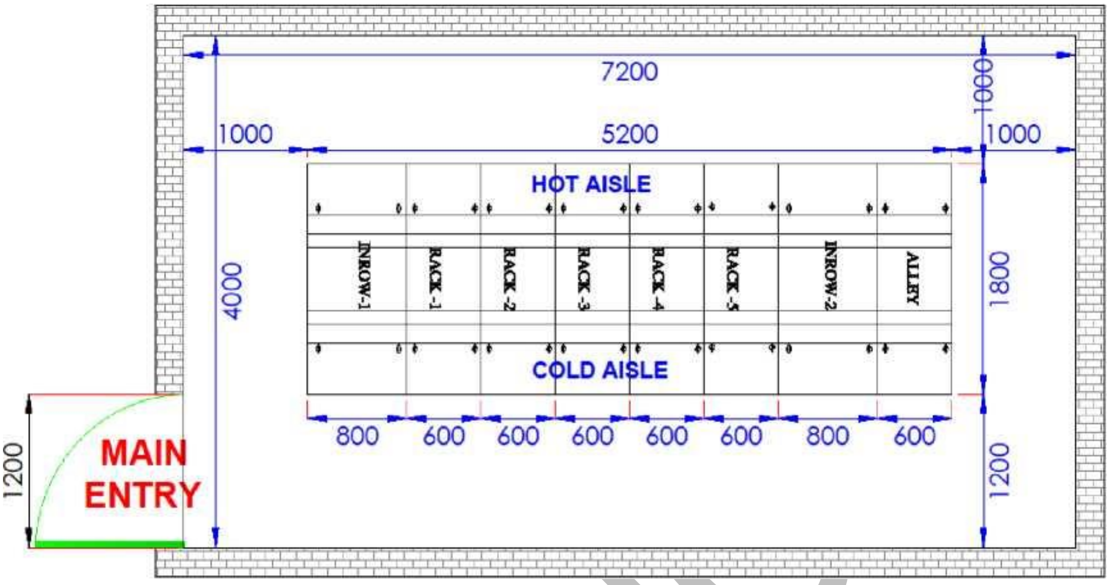
48.3. **Lightining arresters**. Lightining protection system complying with recognized safety standards of LPI175, NFPA780 and UL96A to be installed in the data Centre to avoid downtime, outage and service interruption caused by the after effect of Lighting.

49. **High level of Bill of Material**.

Sl.	Item description	Qty	UOM
49.1	NLDC Civil, Electrical and Interiors	1	Set
49.2	NLDC In-Row Cooling Solution	1	Set
49.3	Building Air conditioning	1	Set
49.4	Modular UPS as per above defined capacities with Lithium-ion batteries for server room	2	Set
49.5	Fire Alarm & NOVEC 1230 based Gas Suppression System	1	Set
49.6	Rodent Control System	1	Set
49.7	Water Leak Detection System	1	Set
49.8	DCIM Software & Accessories (Complete Solution as required)	1	Set
49.9	Environment Management System (EMS) & Accessories (Complete Solution as required)	1	Set
49.10	Biometric Door Access System (as required)	1	Set
49.11	IP Dome Surveillance Camera (as required)	1	Set
49.12	Portable Fire Extinguisher (as required)	1	Set
49.13	DG Set 100KVA with AMF	2	No.
49.14	Server Racks of 10kW (as required)	5	No.
49.15	IT infrastructure sizing and detailed technical specifications as per Chapter-06 of RFP/ IT infrastructure detailed technical specification	1	Set
49.16	Structured Cabling	1	Set

50. **NLDC layout**

Near Line Data Centre Layout



AREA- 28.8SqrM (310Sqrft)

Figure 5-A: Near Line Data Centre - Power distribution Main SLD

51. **Power Distribution- Main SLD**.

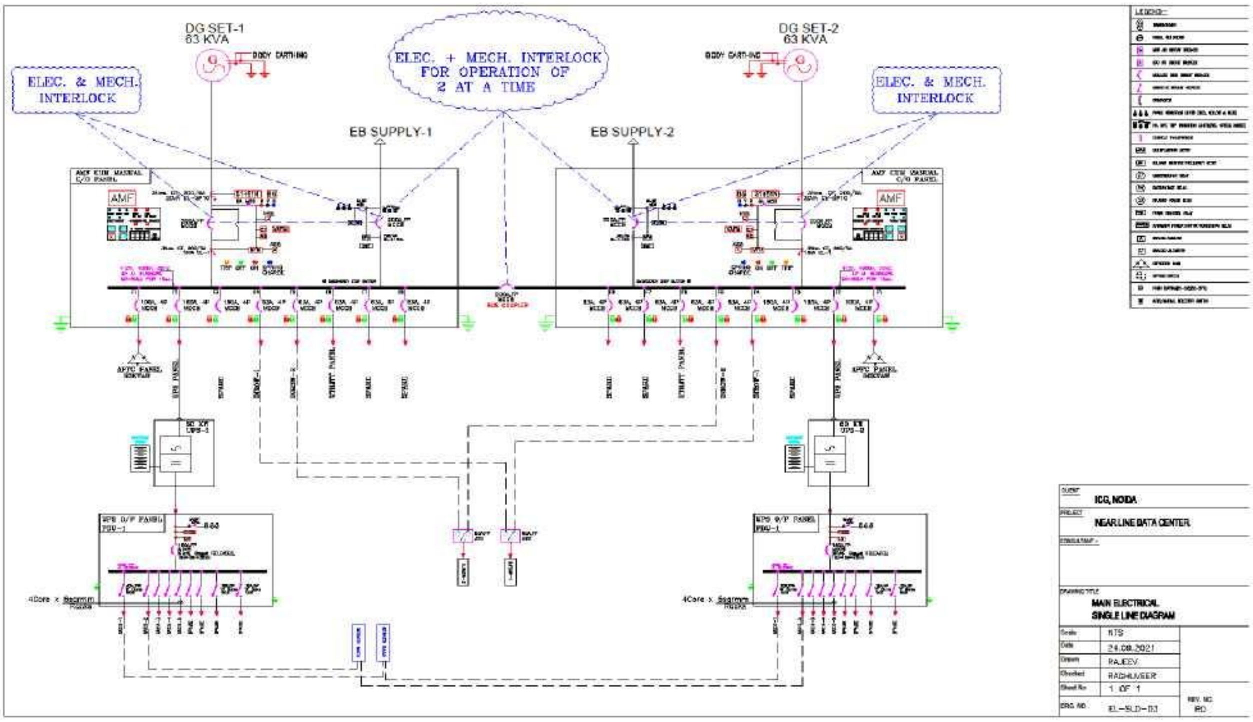


Figure 5-B: Near Line Data Center

VERIFIED

COMPLIANCE OF TECHNICAL SPECIFICATION - DC/ DRDC/ NLDC COMPONENTS

52. C01 - Cloud Management Platform (Includes Service Catalogue, automation & Orchestration, Operations, CI/CD tool)

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
52.1	Automation, Orchestration & Service catalogue	The solution should provide unified and centralized software defined platform that integrates market leading compute, storage, networking and security virtualization and Kubernetes into a common platform to deliver enterprise-ready cloud infrastructure for the private and public cloud.	
52.2		The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, configuration of virtual storage, virtual network, and cluster creation and provisioning.	
52.3		The management components of the solution should have high availability that allows nondisruptive operation of the running workloads.	
52.4		The solution should be able to automate provisioning of data-Centre services such as compute, storage, networking (switches, routers etc), load balancing, firewall, etc. It should have an advanced Blueprint designer for creating virtual machines, application stack blueprints with the ability to release them as catalogue services.	
52.5		The solution shall provide a unified web-based multi-tenant self-service catalogue for IaaS, PaaS and Anything-as-a-Service across virtual and physical platforms.	
52.6		The solution should have a powerful orchestrator to automate complex IT tasks, including integration with existing tools, infrastructure and processes using API calls. It should also provide blueprint version control and sync with private GIT code repositories.	
52.7		The solution should provide capabilities for creation of services such as 'Single VM' and a 'Multi- tier' infrastructure including software-	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
		based constructs such as load balancers as part of a standard template.	
52.8		The solution should provide role base access control using standard authentication and authorization directories like Active Directory (AD) over LDAP, AD with integrated windows authentication and Secure LDAP and allow importing existing users and groups.	
52.9		The solution should be able to Auto Scale-Out/In virtual machines based on their resource utilization such as CPU, RAM usage	
52.10		The solution should support scalable and highly available architecture with deployment on open, extensible architecture with multi-vendor hardware support.	
52.11		The solution should be able to set up multiple tenants or organizations. Each tenant should be able to use its own projects, blueprints, resources and deployments with support for Central SSO, delegated SSO and standalone SSO as required.	
52.12		The solution should provide a web-based automated self-service catalogue for IT/Business users to request for services. It should act as a central point for accessing customised services based on user roles.	
52.13		The solution should provide configuration of approval workflows with support for multiple approval levels along with email notifications sent to approvers so that approvals/rejections can be done without having to login to the self-service portal	
52.14		The solution should provide a comprehensive Swagger/Open API based API reference so that third party services can interact with the solution to provision resources across environments.	
52.15		The solution should provide automated discovery and onboarding of existing resources like compute, network, storage across virtualized environment under management.	
52.16		The solution should support ready integration with software delivered networking & security to provide automated delivery of services such as switching, routing, load balancing and firewalling	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
52.17		The solution should provide service authoring capabilities that includes a graphical drag and drop canvas and also a YAML code editor. It should provide capabilities to design cloud-agnostic full service blueprints and the ability to export/import service blueprints from multiple cloud providers, for e.g., CFT templates, HELM charts etc.	
52.18		The solution should provide the ability to manage the lifecycle of deployments i.e. Change Lease, Delete deployment, Power On/Off and Update the deployment as a Day 2 action.	
52.19		The solution should provide Day 2 operations capabilities to authorised users to start/stop/suspend virtual machines, take snapshot, delete machine, request additional resources and connecting to console through the self-service portal.	
52.20		The solution should provide out of the box integration with Configuration Management tools like Terraform/Ansible Tower/Puppet Enterprise and IP Address Mgmt. like Infoblox etc.	
52.21		The solution should provide the administrators an option to work with it programmatically using the REST API	
52.22		The solution should provide the ability to include lease policies in order to automatically reclaim resources after the specified period of lease and the ability to send notifications to the user when the lease is about to expire so that it can extended.	
52.23		The solution should have the ability to place metadata tags in the form of key-value pairs on resources in order to enforce placement decisions during deployment, associate with policies and run reports pulled on the basis of a metadata tag.	
52.24		The solution should have the ability to create custom workflows to automate the delivery of anything as a service for example Email as a Service, Backup as a Service, AD as a service etc.	
52.25		The solution shall include multiple levels of organizational grouping at Tenant/Business Group/Project level to allow authorized administrators or users service entitlement by role, to request IT services, provide access to	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
		specific resources/clusters, while ensuring compliance with organizational policies.	
52.26		The solution should enable administrators to access Kubernetes clusters so that they can add and create Kubernetes components to support management of containerized applications.	
52.27		The solution should allow addition and management of the configuration of Kubernetes clusters and namespaces which serve as the basis of Kubernetes deployments.	
52.28		The solution should specify what clusters are available for provisioning of Kubernetes namespaces and, additionally, what properties are acceptable for clusters and define policy-based placement of Kubernetes clusters and namespaces	
52.29		Should support Multi-Cloud environment based on OpenStack and provide integration for Service Catalogue services. Should support Multi-Tenant with delegated Tenant specific Cloud Administrators	
52.30		The cloud management platform must provide a seamless integration with the virtualization layer. The solution should be tightly coupled with the virtualization layer and provide a single support window for complete cloud management solution including virtualization and network stack.	
52.31	CI CD	The Solution should automate the release process at each stage of the software delivery pipeline to assure speed and consistency. It must integrate with leading Open source middleware for CI/CD and Enterprise COTS software development, testing, artefact management and build systems to orchestrate tasks that need to be performed in the development process. Software development, testing, artefact management and build systems to orchestrate tasks that need to be performed in the development process.	
52.32		The solution should integrate with source and version control tools and also provide the ability to distribute these artefacts between different tenants	
52.33		The solution should be able to track artefacts and automate deployment configurations to ensure correct versions are used across all stages of the	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
		development lifecycle.	
52.34		The solution should provide real-time visibility into any software release process of in progress pipeline using consolidated dashboards and reports.	
52.35		The solution should support modelling and resolution of artefacts to retrieve the right artefact versions to fed to the correct development scripts or tools when deploying a particular build version of an application.	
52.36		The solution should monitor pipeline status, trends, metrics, and key indicators to identify problems in continuous integration and continuous delivery pipelines.	
52.37	Operations	The operations management solution must provide a seamless integration with virtualization layer	
52.38		The solution should have the capabilities for customization of dashboards and provide customized reports.	
52.39		The solution should have AI/ML driven VM resource reclamation capability which consumes metrics to identify the resources to be reclaimed. It should also provide utilization reports such as over/under utilization and reclamation recommendations along with automated reclamation capabilities.	
52.40		The solution should allow achieve optimal workload management from initial deployment, ongoing rebalance, to retirement and reclamation with complete lifecycle management.	
52.41		The solution should provide Smart Alerts, Root-cause analysis, guided remediation and industry standards compliance evaluation to deliver recommendations, or trigger actions, that optimize performance and capacity and enforce configuration standards.	
52.42		The solution should be able to aggregate and analyse all types of machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps and can be visualized from a single operations console.	
52.43		It should provide an intuitive GUI-based interface that makes it easy to run interactive searches as	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
		well as deep analytical queries for quick, actionable insights.	
52.44		The solution should have capabilities to perform Log retention and Log archival for future access.	
52.45		The solution shall provide a unified management of performance, capacity and compliance for the proposed platform. It should provide the ability to provide ready reports and dashboards for monitoring purposes with identification capability on over-sized, under-sized, right sizing, idle and powered-off VMs, orphaned disks and old snapshots.	
52.46		The solution should provide capacity analytics to do "What If" scenarios such as Project planning to identify the resource shortfall and do Capacity Planning for Future workload requirements.	
52.47		The solution should be able to provide Cost optimization by identifying private cloud reclamation opportunities.	
52.48		The solution shall have built-in high-availability and data replication across its peer instances. In case of any node outage, other HA nodes should be able to take over for seamless HA for the operations management layer itself	
52.49		The solution shall provide the ability to identify and report on over-sized, under-sized, idle and powered-off virtual workloads so that the environment can be right-sized and resources can be reclaimed	
52.50		The solution shall provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements	
52.51		The solution shall provide alerts with symptoms and recommended actions for known problems with the ability to add custom alerts	
52.52		The solution shall have out of the box reporting features for current capacity usage, potential optimizations, physical resource availability, available headroom for expansion and system compliance to security/operational guidelines	
52.53		The solution should give explanations and recommended solutions to performance, capacity and configuration problems. It should be possible to associate workflows with alerts to	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
		automatically initiate corrective measures at critical thresholds	
52.54		The solution should provide prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements	
52.55		The solution should provide the ability to balance workloads across clusters of hosts for optimum usage of resources from a capacity & performance standpoint	
52.56		The solution should support the ability to integrate data from third-party systems to manage the data-Centre ecosystem components such as compute, networking, storage, security, applications and databases.	
52.57		The solution shall pre-emptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times	
52.58		The solution shall provide configuration compliance reports/alerts/dashboards for the underlying hypervisor platform	
52.59		The solution should provide resource reclamation functionality which identifies and reclaims inactive and abandoned resources by automating the decommissioning and reuse of retired resources. It should also provide reclamation savings reports which would enable organizations to quantify its cost savings	
52.60	Log Analytics	The log management solution should have out of the box integration with operations manager in order to better co-relate incidents happening at the data Centre.	
52.61		The log management solution should allow connecting to data-Centre ecosystem components e.g., operating systems, applications, servers, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyse logs at scale.	
52.62		The log management solution should provide intelligent log analytics to be able to bring unstructured and structured data together, for enhanced end-to-end operations management.	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
52.63		The log management solution should be able to collect and analyse all types of machine-generated log data, for example, network traces, configuration files, messages, performance data, system state dumps, and more.	
52.64		The log management solution should be able to add all types of structured and unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand.	
52.65		The solution should have capabilities to perform long term Log retention and Log archival for future access.	
52.66		The solution should export logs to SIEM solution provided, and shall have SIEM native integration for advanced analytics.	
52.67	Cloud Billing	The solution should help cloud administrators define and assign a pricing policy for calculation of the cost of individual deployments to help manage resources within the projects.	
52.68		The solution should include the price of a deployment over time as month-to-date price and must include the component cost breakdowns such as CPU, Storage etc. as available in the deployment details.	
52.69		The solution should be able to provide benchmark cost information for a catalogue that includes a virtual machine with a disk, so as to view the deployment cost.	
52.70		The solution should provide a reference cost for resources and have the ability to configure cost drivers for these resources, basis which the solution should automatically calculate accurate cost for the environment.	
52.71		The solution should have the ability to include standard depreciation methods, like straight line and max of double or straight, and depreciation period from two to seven years.	
52.72		The solution should provide the projected cost of private cloud for the current month and the trend of total cost over time. It should also display the monthly trend of the cost variations, the actual expense, and a chart that represents the actual expense and the reference cost of the expense.	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
52.73		The solution should be able to calculate cost daily and whenever there is a change in the inventory or cost drivers. The cost calculation could also be triggered manually so that changes in the inventory and cost driver values reflect accurately without waiting for the cost calculation process.	
52.74		The solution should provide a predefined cost dashboard for comparing the cost of cloud infrastructure and analyse results in order to identify opportunities to manage the cloud resources efficiently.	
52.75		The solution should provide a predefined cluster cost report to know the total investment on the cluster, the characteristics of the cluster, which datastore the cluster belongs to, and the total capacity of the number of hosts.	
52.76		The solution should provide a predefined datastore cost report to know the total datastore capacity, to which data-Centre the datastore belongs, and the total cost associated with the datastore.	
52.77		The solution should provide a predefined server cost report to know the cost associated with the host, model of the host, and total capacity of the host.	
52.78		The solution should provide a predefined Virtual Machine Cost Report to know the cost associated with the virtual machine, total capacity of the virtual machine, and to which datastore the virtual machine belongs.	
52.79	Orchestration	The solution should provide a development and process-automation platform that provides an extensive library of workflows and a workflow engine.	
52.80		The solution should include a pre-configured orchestrator or integrate with an external orchestrator instance so that workflows can be used as part of extensibility.	
52.81		The solution should provide the flexibility to manage workflow development and object inventory using Git	
52.82		The solution should support the following scripting languages: PowerShell, Node.js, and Python.	

Req. Sl.	Category	C01-Cloud Platform Technical Requirements	Compliance Yes/ No
52.83		The solution should provide a standard library of workflows that can be used to automate operations in the virtual infrastructure	
52.84	Service Catalogue	The solution should have predefined ready to use Service Catalogue for consumption of cloud services including support for Multi-Cloud on OpenStack & NIC Public Cloud	
52.85		The solution should have Life Cycle Management Work flows: Provisioning	
52.86		The solution should have Life Cycle Management Work flows: Decommissioning	
52.87		The solution should have Life Cycle Management Work flows: Capabilities to allow day 2 operations work flows like start/stop/suspend virtual machines, take snapshot, delete machine, request additional resources and connecting to console through the self-service portal	
52.88		The solution must be able to allow administrator or cloud operator define IaaS, PaaS, CaaS and SaaS in the service catalogue for the cloud	

53. **C02 - Compute Virtualization**

Req. Srl	Category	C02 - Compute Virtualization	Compliance Yes/ No
53.1	General	Sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security.	
53.2	OS Support	Must be support all leading Operating Systems.	
53.3		Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.	
53.4		Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.	

Req. Srl	Category	C02 - Compute Virtualization	Compliance Yes/ No
53.5		Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	
53.6		Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software.	
53.7		It should support affinity and anti-affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated.	
53.8		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.	
53.9		Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.	
53.10		Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.	
53.11		Support for persistent memory, exposing it as block storage or as memory, to enhance performance for new as well as existing apps	
53.12		Should be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
53.13		Should support network and storage QoS to ensure performance on per VM basis	
53.14		VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and live virtual motion and also provides secure boot for protection for both the	

Req. Srl	Category	C02 - Compute Virtualization	Compliance Yes/ No
		hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.	
53.15		Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions. Hypervisor to support both agentless security and agent-based security.	
53.16		Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.	
53.17		Span across a virtual datacentre and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.	
53.18		In-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
53.19		Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.	
53.20		Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data Centre with single click	
53.21		Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications	

Req. Srl	Category	C02 - Compute Virtualization	Compliance Yes/ No
		running in primary environment.	
53.22		It should include proactive smart alerts with self-learning performance analytics Capabilities with Prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.	
53.23		Capacity analytics which can identify over-provisioned resources so they can be right-sized and "What If" scenarios to eliminate the need for spreadsheets, scripts and rules of thumb, as well as Real-time, integrated dashboards of performance and capacity to enable a proactive management approach and help ensure SLAs are met	
53.24		Automated workflow triggers which would let admins associate workflows created in Orchestrator layer with Operations alerts. For example, these workflows can automatically delete old VM snapshots when available capacity falls below a critical threshold or add resources when workload demands are rising above normal.	
53.25		Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management.	
53.26		Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.	
53.27		Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.	
53.28		Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.	

54. **C03 - Network & Security Virtualization**

Req. Sl.	Component Name	C03 Network & Security Virtualization Technical Requirements	Compliance Yes/ No
54.1		The SDN solution should be embedded in-kernel highly programmable through APIs integration from a central management point and can be integrated with major industry software management / cloud tools to automate end users' service requests.	
54.2		The solution should provide distributed routing so that routing between Virtual Machines with different IP subnets can be done in the logical space without traffic going out to the physical router thus reducing number of hops	
54.3		Provisioning of virtual/software defined network services should be possible irrespective of make and topology underlying physical network switches and routers and should be capable of supporting major hardware OEMs like Juniper, Arista, Cisco, HPE, Dell.	
54.4		The solution should have capability to extend overlay based network (VXLAN/ Geneve) to a traditional VLAN based network so that an application can seamlessly run across either of the networks without requiring an IP change.	
54.5		The solution should support multi-tenancy and should have inbuilt NAT functionality so that overlapping ip addresses can be used across multiple tenants.	
54.6		The Solution should offer a centrally managed distributed stateful firewall to provide micro-segmentation full stateful L4 to L7 firewall without requiring additional components for the environment. The Security policies can be defined on constructs such as IP address, VM names, vCentre objects and tags, active directory groups, Security tags etc must follow the VM in the event of migration within the data centre.	
54.7		The solution should offer Layer-2 VPN allows you to extend your data centre by allowing virtual machines to retain network	

Req. Sl.	Component Name	C03 Network & Security Virtualization Technical Requirements	Compliance Yes/ No
		connectivity across geographical boundaries.	
54.8		The solution should provide inbuilt L2VPN and L3VPN.	
54.9		The Solution should provide an integrated server load balancer to provide the load balancing functions in a virtual form factor.	
54.10		The solution should offer extending Layer-2 overlay across multiple sites, so that same subnet is available across these sites for configuring virtual machines.	
54.11		The solution should provide option for securing virtual machines with offloaded anti-malware and HIPS solutions without the requirement of agents deployed inside the virtual machine by integration with leading 3rd party anti-malware/HIPS solutions.	
54.12		The solution should support reduction in Recovery Time Objective by allowing the virtual machines to retain the same ip address after migration from DC to DR, the default gateway router should be stretched across datacentres, and also the firewall policies should also be applied across DC & DR.	
54.13		The solution should support auto scale out and scale in functionality so that when traffic load increases, required load balancer instances are added or deleted on demand.	
54.14		The solution should have capability to provide stateful micro-segmentation for diverse workloads covering virtual machines, containers and bare metal servers from a single console.	
54.15		The solution should have integrated distributed IDS functionality for East-West traffic in order to detect malicious traffic.	
54.16		The solution should provide a distributed context aware firewall which provides visibility into the application layer and should be able to block the application irrespective of the port it is using. It should also provide inbuilt FQDN/ URL whitelisting capabilities.	
54.17		The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the	

Req. Sl.	Component Name	C03 Network & Security Virtualization Technical Requirements	Compliance Yes/ No
		purpose of implementing a zero trust security within the data-centre	
54.18		The solution should be able to report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacentre	
54.19		The solution should provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should be capable of integrating with leading hardware OEMs to provide this visibility	
54.20		The solution should provide network & security analytics and should be able to quickly point out top talkers, elephant flows, outliers etc in the environment. It should be capable to provide visibility across Kubernetes/ container environment as well.	

55. **C04 - Container Management Platform**

Req. Sr.	Category	C04 - Container Management Platform	Compliance Yes/ No
55.1	General	Container Platform should support key Open Source tools providing the latest version of pure, upstream Kubernetes based multi container application orchestration on native docker format container images.	
55.2		The Container management solution should be supported on both on-prem on Type-1 hypervisor and prominent public clouds for a consistent multi-cloud experience.	
55.3		The Container management solution however should support burst-out workloads into public/hybrid cloud when the primary site's compute capacity is maxed out or reach a pre-defined threshold.	
55.4		The Container management solution should provide a consistent infrastructure, operations and interfaces (APIs, CLIs and UIs) for operations on both private and public/hybrid cloud.	

Req. Sr.	Category	C04 - Container Management Platform	Compliance Yes/ No
55.5		The solution should be designed to support optimal utilization of compute resources, at times when there are no or minimum load. Those compute resources may be destroyed easily (by scaling down) to make room for more capacity wherever needed within the private cloud.	
55.6		The preferred Container orchestration technology is Kubernetes; the Container management solution should fully support it by providing tested and signed binaries of the Kubernetes and dependent core components.	
55.7		The container platform should support deployment and orchestration multiple containers formats (for e.g. docker etc.) for preventing any technology lock-in.	
55.8		Container Platform should provide a true polyglot platform or similar solution that supports multiple programming languages and enterprise middleware services.	
55.9		The solution should support both container-native applications, as well as non-native applications.	
55.10		Container Platform should be able to configure container health and readiness checks.	
55.11		Container Platform should support the Kubernetes workloads like 1. Replicate Set 2. Replication Controller 3. Deployments 4. Stateful Sets 5. Daemon Sets 6. Jobs 7. Cron Job	
55.12		Container Platform should be able to host both Stateless and Stateful application set	
55.13		Container Platform should be supported on latest technology.	
55.14		Container Platform should have service discovery capability through Kubernetes services with integrated DNS. Kubernetes services can proxy scaled containers as well as a user defined heterogeneous set of containers	
55.15		The solution should provide support to	

Req. Sr.	Category	C04 - Container Management Platform	Compliance Yes/ No
		integrate with existing AD or LDAP for Auth N/Z and RBAC for Cluster level and Image registry.	
55.16		Container Platform should integrate with Cloud Management Portal providing visibility into VMs and Containers with automated policy management.	
55.17		Proposed solution should be able to expand additional resource on the fly without interruption to existing deployment.	
55.18		The Solution should be capable to determine optimal number of containers fits with the environment.	
55.19		The Solution should be capable to scale the application deployment up and down based on resource utilization (CPU, memory)	
55.20		The solution should be capable of automatically keep application cluster up to date with the latest release version of container-orchestration system.	
55.21		The solution should be able to support rollback deployment.	
55.22		The solution should support environmental consistency across development, testing and production.	
55.23		Solution should provide rest API to that exposes operations for managing a cluster, security and user management, application deployments, image and source builds, HTTP(s) routing and project management.	
55.24		The solution should provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking services at Layer 2 through 7 such as DNAT/SNAT, DHCP, Load Balancers (L4 and L7) and firewall in addition to switching and routing (North-South and East-West).	
55.25		The solution should support Routable Pods in addition to NAT'd Pods. The IP addresses of some or all Pods in a network should remain unchanged while making an egress connection outside of the Kubernetes Cluster.	
55.26		Solution Should implement the Kubernetes APIs i.e. 'Network Policy', 'Ingress' and 'Load Balancer' constructs to support Distributed	

Req. Sr.	Category	C04 - Container Management Platform	Compliance Yes/ No
		Firewalling, Pod level micro-segmentation and access to Service.	
55.27		The solution should integrate with Kubernetes to provide app-deployment automation via cloud-native L4 Objects (Kubernetes Services)	
55.28		The solution should automatically track backend Pod lifecycle changes (deletion and recreation of application Pods) and update the Load balancer pool appropriately without user intervention.	

56. **C05 - Windows Server License.** Windows Server Data Centre edition licenses as per the solution requirement. Minimum requirement is given in Bill of Material.

57. **C06 - Linux Server Enterprise License.** Linux server enterprise edition licenses/ subscription as per the solution requirement. Minimum requirement is given in Bill of Material.

58. **C07 - Composable IT Infrastructure**

Sr.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
58.1	General Requirements	Composable IT Infrastructure	
58.2	Stateless resource pool	Disaggregated resource control to enable ability to independently scale resources including memory, storage, compute and network	
58.3		Compute, storage and networking resources should be stateless, separated from underlying physical infrastructure and independent of each other	
58.4		Proposed solution should support heterogeneous platforms, Open stack hypervisors and next generation containers and Bare metal servers concurrently on the same cluster	
58.5		Solution should provide the flexibility to combine the compute and storage functions on the same hardware along with option of separate the compute and storage	

Sr.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
		functions into different tiers. Irrespective of the mode of deployment, the hardware solution should be managed using a single GUI	
58.6		Should provide unified single GUI to manage stateless resource pool	
58.7	Scalability	Proposed solution should be scalable upto 150 nodes in a single management cluster, scalable to multiple management clusters having minimum of 1000 nodes.	
58.8		Linear scalability of IT resources	
58.9	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	
58.10		Enables developers to programmatically deploy new virtual machines and other structures so that they can more quickly test their code	
58.11		Allows an application to automatically instantiate new infrastructure based on performance conditions at the present time	
58.12		Enables automation-based user self-service, and support 'Private Cloud' services	
58.13		Support DevOps	
58.14	OEM ERP Certification	Should be certified for deployment by OEM of ERP application instance being offered to ICG	
58.15	SDDC Support	Should support Software Defined Data Centre (SDDC), detailed requirements are as defined in succeeding specifications	
58.16		The solution should support 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	

Sr.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
58.17	Support	Hardware support to be from the same, single OEM and not outsourced from any third party, either licensed or non-licensed	
58.18	Unified REST API	Provide Unified REST API interface to enable the automation of operations	
58.19	Compute Node	(a) 2 socket x 24 Core, 2.2 GHz per Node or higher (b) Intel Xeon Gen10 or latest (c) Processor cache 35 MB or higher (d) 1024 GB DDR4-2666 or higher (d) SSD, 6/12 G (e) Memory should feature Advanced ECC, Memory Mirroring Mode and adaptive double device data correction / Memory Online Spare (f) Silicon Root-of-Trust inbuilt into System-on-Chip	
58.20	Storage Node Controller	(a) Support minimum of 24 SFF of 12G SAS/ 6G SSD (b) Capacity to be scalable upto 100 TB or higher per node (c) Storage be provided in SAS HDD	
58.21	Compute requirement	(a) The compute configured should have minimum Spec Int Ratings Base 337 - CPU2017 or better (b) Each compute node should deliver minimum 75000 SAP Count/ equivalent at 65% CPU Utilization or equivalent	
58.22	Data Protection	Compute node should have dedicated cache in raid controller for data protection	
58.23	Power Supply	High-efficiency, hot-plug, Platinum Efficient redundant power supplies	
58.24	OS Support	All latest Operating systems.	
58.25	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	
58.26	Management	(a) Should be provided along with server from server OEM only	

Sr.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
		(b) Agent Free monitoring (c) Should support for Virtualization platform (d) IPMI 2.0 or above/ latest in vogue	
58.27	OEM Warranty	Warranty of 05 years from the date of installation for hardware, software including required cloud virtualisation software	
58.28	SI Warranty, AMC for integration support	(a) Warranty SI to obtain required L3 level support from Cloud Virtualisation Software for integration towards commissioning, warranty & AMC period support. SI to renew L3 support with OEM with no additional financial implication from the Buyer (b) SI to obtain required L3 level support from OEM for integration towards commissioning, warranty & AMC period support.	

59. **<u>C08 - Rack Server</u>**

Sl.	Category	Technical Requirements for Rack Server	Compliance Yes/ No
59.1	Compute	(a) 2 socket x 18 Core, 3.0 GHz per Node or higher (b) Intel Xeon Gen 9 or latest © Processor cache 25 MB or higher (c) 1024 GB DDR4-2666 NVDIMM or higher (d) Minimum SSD 2x250GB, 12 G © Memory should feature Advanced ECC, Memory Mirroring Mode and adaptive double device data correction / Memory Online Spare	
59.2	Storage	(a) Support minimum of 04 SFF 12G SAS/ 6G SSD (b) Capacity to be scalable upto 100 TB or higher per node	
59.3	Network	(a) Provide FC-HBA in High Availability with SAN Switch (b) Provide Ethernet ports in HA as required	

59.4	Other Software	(a) Windows 2016 Server DC Edition or latest with SA (b) Backup software, 10 VM or 02 Socket © Endpoint Protection Software – 01 No. (d) Virtualisation software – 02 Socket	

60. **<u>C09 – Block and File Storage – Intranet</u>**

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
60.1	Data Availability and All Flash	Offered solution shall be a 99.9999% (six nine's) data availability guaranteed architecture and All Flash array only. Shall be marketed / Published as All Flash array on the vendor web site.	
60.2		99.9999% (six nine's) data availability guaranty shall be clearly mentioned on vendor web site for the offered model.	
60.3	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including: Windows Server 2016, VMware, Solaris and HPE-UX etc.	
60.4	Capacity & Scalability	Offered Array shall be scalable to at-least 2000 TB native raw capacity on all Flash using drives in a single storage system	
60.5		Offered storage solution shall support at-least 240 e drives. Proposed system to be configured in such a way that only enclosures and NVMe drives would be required to meet the capacity and drive scalability mentioned above.	
60.6		Offered Storage array shall be supplied minimum with 60TB Capacity using 3.84 TB drives and shall be configured in Raid 6 or equivalent excluding all overheads like RAID parity, file system etc.	
60.7	Storage Encryption	Vendor shall offer drives with appropriate encryption licenses and shall meet FIPS 140-2 – Level 2 security requirements. Vendor shall also offer controller based or Software based encryption.	
60.8		Storage array must support data-at-rest encryption in compliance with FIPS 140-2 certification managed by On-board Key Manager or External Key Manager using a cryptographic security module.	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
60.9	No. of Controllers	Offered Storage shall be supplied with at-least Dual Symmetric Active/Active controllers where all the volumes and LUN’s shall be active from all the controllers and shall be scalable to at-least Four controllers. The storage should support natively FC, NVMe-of, iSCSI, NFS (NFSv3, NFSv4), CIFS/SMB protocols for use with different applications. Bidder needs to propose minimum dual NAS controller incase offered system doesn't natively support NAS functionality.	
60.10		A failure of controller should not lead to write-through mode for cache.	
60.11	Cache and CPU Processing Power	Offered Storage array should have at-least 1024GB cache and shall be scalable to at-least 3TB by DiP controllers in the same storage.	
60.12		Offered storage shall be based upon Intel/AMD CPUs minimum cascade lake series, and shall be supplied with at-least 40 numbers of CPU cores, Scalable to 80 CPU cores by adding multiple controllers.	
60.13	Processing Power & Scalability-	Offered Storage shall support effective handling of NVMe parallelism, Raid-Rebuilding and data striping, thin re-claim etc.	
60.14		Storage array shall be scalable to at-least 4 dedicated controllers in same storage.	
60.15		In case vendor doesn’t have above functionality to scale for balancing the performance then additional 32 CPU cores shall be provided.	
60.16	Security & Data Protection	The storage array should have support for controller-based snapshots (At-least 1000 copies for a given volume). Storage Array shall have functionality to create virtual lock for retention of read-only snapshots to protect against accidental deletes and Cybercrime incidents.	
60.17		Storage management software should support MFA to ensure secure access of Management Software. The Storage array should support SHA-2 level security for managing user credentials.	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
60.18	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure for the offered configuration including Array Controller card, Cache memory, FAN, Power supply etc.	
60.19	Monitoring and Analytics	Providing Firmware upgrade and patch upgrade recommendations proactively and with awareness of the peripheral infrastructure connected to the array.	
60.20		Providing extremely granular historical capacity and performance trend analysis by default, without the need to enable extra logging, install any appliances (physical or virtual), or install any software.	
60.21		Providing overall saturation level of the array while analyzing various parameters like IOPS, MB/sec, Block size etc. Quality of Service feature configured for both min and max limit for required IOPS / bandwidth at individual volume/LUN. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time. Any additional license should be configured for the same if required.	
60.22		Providing overall performance of the array for both read and write operations.	
60.23		Shall provide history of support cases logged with Support team under different column like Critical, Normal and low severity along with closed cases. Cloud monitoring tool shall be able to provide the complete month-wise breakup.	
60.24		Shall be able to provide the executive Dashboard covering various critical and must aspects of Total Capacity, overall health / wellness of array. De-duplication and compression ratio, over-all front-end performance etc.	
60.25	Hyper Visor Integration	monitoring and analytics engine integration with Hypervisor	
60.26		Offered monitoring and analytics engine shall be integrated with Hypervisor layer and shall be certified to work with at-least VMware.	
60.27		The proposed storage should enable and	

VERIFIED

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		integrate with server virtualization technologies such as VMware vSphere. The proposed storage must support VASA 3.0 and above, VMware VVOL feature and feasibility to create more than 5000VMs using VVOLs. The proposed array should be able to present both VVOL storage pool and traditional LUN's. Shall support both compression and de-duplication for VVOL	
60.28	Analytics - Performance	Shall have panel which can depict the overall saturation/ utilization level of the storage array at different time intervals instead of looking into individual parameters like IOPS, CPU utilization, Cache utilization etc.	
60.29		If similar nature of arrays being used in the environment then offered engine shall show the top/multiple systems within the same console.	
60.30	Data Protection	System should offer capability to protect the write cache in case of a controller failure storage subsystem shall have de-staged mode so that un-committed information can be protected. De-staging shall happen to redundant vault drives and vault drives shall be encrypted. Also, a failure of controller should not lead to write-through mode for cache.	
60.31	Host Ports and Back-end Ports	Offered Storage array shall have minimum of 16 x 32Gbps Fiber Channel ports and 16 x 10G ports shall be scalable to at-least 48 x 32Gbps Fiber channel ports across controllers	
60.32		Offered Storage array system shall be supplied with two x 10Gbps additional native IP ports per controller for storage based replication.	
60.33		Offered Storage array shall have NVMe back-end for disk connectivity	
60.34		Offered Storage array shall have minimum of 96 x PCI Gen3 PCI-lanes in the back-end for disk connectivity and shall be scalable to 192 x PCI Gen3 PCI Lanes without replacing the existing controllers	
60.35	Data In place Upgrade - Investment	Offered Storage shall support data in place non-disruptive upgrade to next model of array within the same offered series and	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
	Protection	shall be scalable to at-least 3TB Cache	
60.36	Hot Spare	Offered Storage Array shall provide additional spare capacity as per OEM best practice	
60.37		Global hot spare shall be configure as per industry practice.	
60.38	Quality of service	Offered storage array shall support quality of service for critical applications/volumes so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service/ response time for different application logical units.	
60.39		Quality of service engine shall allow to define minimum and maximum cap for required IOPS/ bandwidth for a given logical units of application running at storage array.	
60.40		It shall be possible to change the quality of service Response time, IOPS, bandwidth specification at real time.	
60.41	Capacity efficiency	Offered storage array shall support inline data efficiency (Supporting Thin Zero detect and re-claim, De-duplication and Compression) The proposed storage should provide in-line efficiency features such as Compression, De-Duplication	
60.42		Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the maximum supported capacity of array.	
60.43		Offered storage array shall be tightly integrated with VMware can be used with thin provisioning and thin re-claim.	
60.44	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	
60.45	Integration - VMWARE	Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL.	
60.46		Offered Storage array VASA provider shall be certified by VMware for VVOL - based replication.	

VERIFIED

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
60.47	Integration - Container	Offered Storage array shall be integrated with Docker, Red-hat OpenShift, Kubernetes container technologies. Vendor shall support at-least following functionalities through their integration CSI / CSP integration plugin:	
60.48		Shall support both Static and Dynamic provisioning	
60.49		Shall be able to create and delete the snapshots	
60.50		Shall be able to expand, re-size the persistent volumes given to state fullest applications.	
60.51		Quality of service for response time, Bandwidth and IOPS.	
60.52		Offered storage array shall be true multi-tenant and shall support more than 512 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.	
60.53		Support for both NFS as well as ISCSI for Containers.	
60.54	Snapshot / Point in time copy	The storage array should have support for controller-based snapshots functionality (At-least 1024 copies for a given volume).	
60.55	Storage Array Configuration & Management Software	Vendor shall provide Storage Array configuration and Management software.	
60.56		Software shall be able to manage more than one array of same family.	
60.57	Remote Replication	The Storage array should be offered with Synchronous, Asynchronous replication feature & Zero Data Loss protection for a volume across 3DC's i.e. between the DC, DR and Near DR	

61. **C10 - Block and File Storage – Internet**

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
61.1	Data Availability and All Flash	Offered shall be a 99.9999% (six nine's) data availability guaranteed architecture and All Flash array only. Shall be marketed /	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		Published as All Flash array on the vendor web site.	
61.2		99.9999% (six nine's) data availability guaranty shall be clearly mentioned on vendor web site for the offered model.	
61.3	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including: Windows Server 2016, VMware, Solaris and HPE-UX etc.	
61.4	Capacity & Scalability	Offered Array shall be scalable to at-least 2000 TB native raw capacity on all Flash using drives in a single storage system	
61.5		Offered storage solution shall support at-least 240 e drives. Proposed system to be configured in such a way that only enclosures and NVMe drives would be required to meet the capacity and drive scalability mentioned above.	
61.6		Offered Storage array shall be supplied minimum with 60TB Capacity using 3.84 TB drives and shall be configured in Raid 6 or equivalent excluding all overheads like RAID parity, file system etc.	
61.7	Storage Encryption	Vendor shall offer drives with appropriate encryption licenses and shall meet FIPS 140-2 – Level 2 security requirements. Vendor shall also offer controller based or Software based encryption.	
61.8		Storage array must support data-at-rest encryption in compliance with FIPS 140-2 certification managed by On-board Key Manager or External Key Manager using a cryptographic security module.	
61.9	No. of Controllers	Offered Storage shall be supplied with at-least Dual Symmetric Active/Active controllers where all the volumes and LUN's shall be active from all the controllers and shall be scalable to at-least Four controllers. The storage should support natively FC, NVMe-oF, iSCSI, NFS (NFSv3, NFSv4), CIFS/SMB protocols for use with different applications. Bidder needs to propose minimum dual NAS controller incase offered system doesn't natively support NAS functionality.	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
61.10		A failure of controller should not lead to write-through mode for cache.	
61.11	Cache and CPU Processing Power	Offered Storage array should have at-least 1024GB cache and shall be scalable to at-least 3TB by DiP controllers in the same storage.	
61.12		Offered storage shall be based upon Intel/AMD CPUs minimum cascade lake series, , and shall be supplied with at-least 40 numbers of CPU cores, Scalable to 80 CPU cores by adding multiple controllers.	
61.13	Processing Power & Scalability-	Offered Storage shall support effective handling of NVMe parallelism, Raid-Rebuilding and data striping, thin re-claim etc.	
61.14		Storage array shall be scalable to at-least 4 dedicated controllers in same storage.	
61.15		In case vendor doesn't have above functionality to scale for balancing the performance then additional 32 CPU cores shall be provided.	
61.16	Security & Data Protection	The storage array should have support for controller-based snapshots (At-least 1000 copies for a given volume). Storage Array shall have functionality to create virtual lock for retention of read-only snapshots to protect against accidental deletes and Cybercrime incidents.	
61.17		Storage management software should support MFA to ensure secure access of Management Software. The Storage array should support SHA-2 level security for managing user credentials.	
61.18	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure for the offered configuration including Array Controller card, Cache memory, FAN, Power supply etc.	
61.19	Monitoring and Analytics	Providing Firmware upgrade and patch upgrade recommendations proactively and with awareness of the peripheral infrastructure connected to the array.	
61.20		Providing extremely granular historical capacity and performance trend analysis by default, without the need to enable extra logging, install any appliances (physical or	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		virtual), or install any software.	
61.21		Providing overall saturation level of the array while analyzing various parameters like IOPS, MB/sec, Block size etc. Quality of Service feature configured for both min and max limit for required IOPS / bandwidth at individual volume/LUN. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time. Any additional license should be configured for the same if required.	
61.22		Providing overall performance of the array for both read and write operations.	
61.23		Shall provide history of support cases logged with Support team under different column like Critical, Normal and low severity along with closed cases. Cloud monitoring tool shall be able to provide the complete month-wise breakup.	
61.24		Shall be able to provide the executive Dashboard covering various critical and must aspects of Total Capacity, overall health / wellness of array. De-duplication and compression ratio, over-all front-end performance etc.	
61.25	Hyper Visor Integration	monitoring and analytics engine integration with Hypervisor	
61.26		Offered monitoring and analytics engine shall be integrated with Hypervisor layer and shall be certified to work with at-least VMware.	
61.27		The proposed storage should enable and integrate with server virtualization technologies such as VMware vSphere. The proposed storage must support VASA 3.0 and above, VMware VVOL feature and feasibility to create more than 5000VMs using VVOLs. The proposed array should be able to present both VVOL storage pool and traditional LUN's. Shall support both compression and de-duplication for VVOL	
61.28	Analytics - Performance	Shall have panel which can depict the overall saturation/ utilization level of the storage	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		array at different time intervals instead of looking into individual parameters like IOPS, CPU utilization, Cache utilization etc.	
61.29		If similar nature of arrays being used in the environment then offered engine shall show the top/multiple systems within the same console.	
61.30	Data Protection	System should offer capability to protect the write cache in case of a controller failure storage subsystem shall have de-staged mode so that un-committed information can be protected. De-staging shall happen to redundant vault drives and vault drives shall be encrypted. Also, a failure of controller should not lead to write-through mode for cache.	
61.31	Host Ports and Back-end Ports	Offered Storage array shall have minimum of 16 x 32Gbps Fiber Channel ports and 16 x 10G ports shall be scalable to at-least 48 x 32Gbps Fiber channel ports across controllers	
61.32		Offered Storage array system shall be supplied with two x 10Gbps additional native IP ports per controller for storage based replication.	
61.33		Offered Storage array shall have NVMe back-end for disk connectivity	
61.34		Offered Storage array shall have minimum of 96 x PCI Gen3 PCI-lanes in the back-end for disk connectivity and shall be scalable to 192 x PCI Gen3 PCI Lanes without replacing the existing controllers	
61.35	Data In place Upgrade - Investment Protection	Offered Storage shall support data in place non-disruptive upgrade to next model of array within the same offered series and shall be scalable to at-least 3TB Cache	
61.36	Hot Spare	Offered Storage Array shall provide additional spare capacity as per OEM best practice	
61.37		Global hot spare shall be configure as per industry practice.	
61.38	Quality of service	Offered storage array shall support quality of service for critical applications/volumes so that appropriate and required response time can be defined for application logical units at	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		storage. It shall be possible to define different service / response time for different application logical units.	
61.39		Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array.	
61.40		It shall be possible to change the quality of service Response time, IOPS, bandwidth specification at real time.	
61.41	Capacity efficiency	Offered storage array shall support inline data efficiency (Supporting Thin Zero detect and re-claim, De-duplication and Compression) The proposed storage should provide in-line efficiency features such as Compression, De-Duplication	
61.42		Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the maximum supported capacity of array.	
61.43		Offered storage array shall be tightly integrated with VMware can be used with thin provisioning and thin re-claim.	
61.44	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	
61.45	Integration - VMWARE	Offered storage array shall be tightly integrated with VMware and shall be certified for VVOL.	
61.46		Offered Storage array VASA provider shall be certified by VMware for VVOL - based replication.	
61.47	Integration - Container	Offered Storage array shall be integrated with Docker, Red-hat OpenShift, Kubernetes container technologies. Vendor shall support at-least following functionalities through their integration CSI / CSP integration plugin.	
61.48		Shall support both Static and Dynamic provisioning	
61.49		Shall be able to create and delete the snapshots	
61.50		Shall be able to expand, re-size the	

Sl.	Category	Block & File Unified Storage Technical Requirements	Compliance Yes/ No
		persistent volumes given to state fullest applications.	
61.51		Quality of service for response time, Bandwidth and IOPS.	
61.52		Offered storage array shall be true multi-tenant and shall support more than 512 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.	
61.53		Support for both NFS as well as ISCSI for Containers.	
61.54	Snapshot / Point in time copy	The storage array should have support for controller-based snapshots functionality (At-least 1024 copies for a given volume).	
61.55	Storage Array Configuration & Management Software	Vendor shall provide Storage Array configuration and Management software.	
61.56		Software shall be able to manage more than one array of same family.	
61.57	Remote Replication	The Storage array should be offered with Synchronous, Asynchronous replication feature & Zero Data Loss protection for a volume across 3DC's i.e. between the DC, DR and Near DR	

62. **C11 - Secondary Storage, Web Scale, SMB/ NFS/ S3**

Sl.	Category	Secondary Storage Technical Requirements	Compliance Yes/ No
62.1	Controllers and Architecture	Storage solution Should be fully clustered Architecture providing true Scale-Out Storage.	
62.2		The Complete multi-controller Storage System Solution should be fully redundant, configured in High Availability clustered mode	
62.3	Onboard Memory	The proposed storage should be a multi controller architecture. With each node/controller should be configured with minimum 192GB DRAM /DDR4 based cache memory for read & write operations.	
62.4	Operating System	Scale-Out Storage should have fully distributed, specialized purposed built SDS (Software Defined Storage) OEM, dedicated for serving data efficiently and customized for True Scale-	

Sl.	Category	Secondary Storage Technical Requirements	Compliance Yes/ No
		Out Storage. SDS should be able to run on any x86 Server Architecture without vendor lock-in's. Software defined scale-out storage vendor shall be listed in Gartner's in 2020/2021 Magic Quadrant for Distributed File Systems and Object Storage as a leader.	
62.5	Hardware Type	Storage solution should have capability to support different kinds of disks types likes SSD/SAS & NL SAS in same storage Cluster. Each controller node Should support Minimum 24 drives or more	
62.6		The Scale-Out Storage System should be able to protect the data against simultaneous 1 (One)disk and 1 Node Failure using Erasure Controller algorithm and should not depend on any RAID based disk subsystem	
62.7		The Scale-Out Storage should be configured to sustain storage controller/ storage node failure in the storage system without data unavailability. Storage system must be offered in a No-Single-Point of Failure offering upto Eight 9s or higher of availability	
62.8		Complete Secondary storage solution has to be from single OEM (including software, OS and hardware).	
62.9	Capacity	2PB usable capacity after considering above mention data protection across min 6 Controller/Nodes Should provide single namespace after required protection level on complete storage solution using NL-SAS hard drives of up to 18TB per disk or less. The storage should be scalable up-to 20PB as a single cluster/file system and up to 100's of nodes. The expansion of secondary storage should support intermixing of multiple node/controllers types, adding drives in the nodes, adding higher capacity drives in the same nodes supporting asymmetric upgrades across sites. Storage must have capability to independently scale for performance and capacity. Proposed storage must provide balancing of the stored capacity across all nodes in a cluster, ensuring data/load gets evenly distributed across all nodes. When new	

VERIFIED

Sl.	Category	Secondary Storage Technical Requirements	Compliance Yes/ No
		nodes are added, data should be redistributed among all nodes. Any change in the connecting topology, like adding the nodes, shall broadcast the change to few nodes instead of broadcasting to all nodes in the cluster. Vendor shall provide the documentary proof that how inter routing mechanism is being done.	
62.10	Network Ports	Provide Minimum 4*10 /25GBps per controller/server node.	
62.11	Protocols	The storage must have open architecture with native support for S3 and support for HTTP/HTTPS, REST, standard POSIX filesystem protocols (Linux filesystems, CIFS, NFS). The storage system shall natively support sharing a single namespace via multiple access protocols (example: ingest a file via NFS and then serve the same file out over HTTP without transforming or copying the data).	
62.12		The solution should provide multiprotocol support NFS, SMB & S3. Storage should support industry standard API like REST, S3, Open Stack, Swift, CDMI for ingest & Object retrieval and should support AD/LDAP integration.	
62.13	Availability, Reliability & Durability	The solution has to provide a minimum of eight nines durability on a Single Site and shall have capability to provide fourteen nines on multiple Site. Offered solution shall be completely redundant and there shall be no single point of failure. Offered solution shall have file integrity checking when reading the file and automatic rebuilt if an error is detected.	
62.14		The storage must support data-at-rest encryption.	
62.15	Storage features	The solution quoted should be scale out and scalability of minimum 100PB	
62.16		There shall be No size limit for object or files which can be stored in the cluster.	
62.17		Offered storage Solution shall be able to scale up to 2^160 object Solution shall offer snapshots and quick recovery capabilities	
62.18		Proposed object storage solution should support custom Meta Data, searching data through these custom meta data Solution shall	

Sl.	Category	Secondary Storage Technical Requirements	Compliance Yes/ No
		provide WORM capabilities to lock.	
62.19		Object storage should be able to support multiple generation of hardware in same cluster Solution should provide search facility across the files to retrieve the files quickly	
62.20		Offered storage shall allow capacity extensions done by adding disks to existing servers (scale-up) or adding additional servers to the system (scale-out). Addition of drives within the same nodes can be of higher capacity to take advantage of Higher density.	
62.21		For better performance, Storage solution shall automatically use Replication factor approach for all files / objects less than 60KB in size. This shall be adjustable, if required.	
62.22		Object interface would be scalable S3. its architecture shall include the following: • S3-Server: S3 API Server for Buckets/Objects, MPU and more • Scale-Out "any-to-any" access • Security model S3-Vault: Security service for Accounts a. Multi-tenant, Support for S3 IAM – Identity and Access Management. b. Authentication with Signature v2 and v4 c. Microsoft Active Directory over SAML 2.0 (ADFS) Integration d. Comprehensive AWS IAM security model for Users & Groups with Roles e. Bucket & Object ACLs • S3-Metadata: Distributed Metadata Engine • S3 Bucket Service Utilization API (UTAPI) + Account level Utilization metrics. • S3 Bucket Versioning • S3 Object Lock • Transparent Bucket-Level At-REST Encryption • Multi-Object-Delete, Website API, CORS API • S3 Stretched deployments for 2 & 3-sites • S3 CRR- Cross Region Replication for asynchronous replication. • S3 Console: GUI Web interface to manage accounts, users, policy and monitor usage.	

Sl.	Category	Secondary Storage Technical Requirements	Compliance Yes/ No
		• S3 Browser: GUI Web interface to create buckets and upload objects. • Quota for S3.	
62.23		Shall be complied solution on various regulations e.g. SEC, GDPR, GoBS, Euro-SOX, AO, Basel III, SOX, HIPAA etc. Offered storage shall ensure that Data must be tamper-proof. Data must be kept for a specified period which means offered storage shall provide retention mechanism. Offered storage shall have capability to migrate the data to an alternative media Offered platform shall be certified by over 80 major ISVs.	
62.24	Replication	Offered storage shall support both Synchronous as well as Asynchronous replication. Shall support Replicating one to many asynchronously so that a given bucket can be replicated to several private and public Cloud targets. Object storage should be able to scale seamlessly and asymmetrically across geographically dispersed data Centres without any reconfiguration of system.	

63. **C12 -Tape Library**

Sl.	Category	Tape Library Technical Requirements	Compliance Yes/ No
63.1	Tape Drive Architecture	Offered LTO-8 drive in the Library shall conform to the Data rate matching technique for higher reliability.	
63.2		Tape Drive Architecture in the Library shall conform to the INCITS/T10 SCSI-3 standard or newer standards.	
63.3	Speed	Offered LTO-8 drive shall support 300MB/sec in Native mode. Shall be offered with min 4 LTO-8 drives.	
63.4	Scalability	Tape Library shall be scalable to more than 500 slots and 40 number of LTO-8 Drives within the same Library.	
63.5	Connectivity	Offered Tape Library shall provide 8Gbps native FC connectivity to SAN switches.	
63.6	Partitioning	Offered Tape Library shall have partitioning support so that each drive can be configured in a	

Sl.	Category	Tape Library Technical Requirements	Compliance Yes/ No
		separate partition.	
63.7		Offered Tape Library shall have support for at-least 20 partition.	
63.8	Management	Tape Library shall provide web based remote management.	
63.9	Encryption device	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.	
63.10	Barcode Reader and Mail slots	Out of 80 slots, Tape library shall support Barcode reader and at-least 5 mail slots and shall be scalable to 30 mail slots when fully populated.	
63.11		Offered LTO-8 drive shall also support LTO-7 – Type M media so that native cartridge capacity of LTO-7 cartridge can be increased to 9TB.	
63.12	Other Features	Tape Library shall have GUI Panel	
63.13		Shall be rack mountable.	
63.14		Shall have option for redundant power supply	
63.15		Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.	
63.16		Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved	

64. **<u>C13 – Back up Appliance</u>**.

Sl.	Category	Technical Specifications - Backup Appliance	Compliance Yes/ No
64.1	General	Offered device shall have capability to deliver selective restore from disk Library itself.	
64.2		Offered Device shall integrate and utilize existing current tape backup infrastructure with ICG in the following aspects (a) Compatibility with the existing backup server / media servers at customer. (b) Compatibility with existing tape library and tape drives (c) Compatibility with existing backup software	
64.3		Offered disk-based backup appliance shall support	

Sl.	Category	Technical Specifications - Backup Appliance	Compliance Yes/ No
		VLAN tagging. Offered IP ports shall also support Port bonding in Adaptive Load balancing as well as in Active-backup mode.	
64.4	Form factor	Offered Disk to disk backup device shall be space efficient and shall not consume more than 2U of rack space.	
64.5	Storage Capacity	Offered device shall be offered with Minimum of 50TB of raw space scalable to 200TB	
64.6	RAID protection	Offered device shall be protected with hardware RAID-6 from the factory so that no raid configuration is required in field.	
64.7	VTL Emulation	Offered device shall support emulation of both VTL and NAS target like CIFS.	
64.8	NAS Target Capacity	Offered device shall have the ability to configure at-least combination of 20 tape Libraries & NAS targets along with 20,000 or more Cartridge slots in the single appliance.	
64.9	De-duplication	Offered device shall have integrated de-duplication license and shall have optional support for replication to remote location in a low bandwidth mode so that only unique – Non Duplicated data flows to remote location.	
64.10		Offered device shall support intelligence for understanding Source based (At Client application level, Backup Server level and media server level) de-duplication so that only unique – Non duplicated data copies to offered device.	
64.11		Offered disk based backup appliance shall have flexibility to enable or disable the de-duplication for a given virtual tape library or CIFS share.	
64.12	Instant Recovery	Instant recovery is a feature that allows customers to mount a file system or start a VM directly from the backup repository	
64.13		Offered device shall support receiving non duplicated data from remote locations or branch office directly from the application servers / Client servers in low bandwidth mode without using any backup or replication based device at remote location / Branch office.	
64.14	Tape format	Ability to flexibly emulate tape drive/ tape formats	

Sl.	Category	Technical Specifications - Backup Appliance	Compliance Yes/ No
	support	LTO-Gen4, LTO-Gen5, LTO-Gen6 and LTO-Gen7 etc.	
64.15	Interface support	Offered device shall have Minimum of 4 x 10Gbps IP, 4 x 8Gbps FC	
64.16	Encryption	Support encryption at Data-in-Rest using AES 256 or higher	
64.17	Performance	Offered device shall support rated write performance, of at-least 25TB/hr.	
64.18	Compatibility	Offered Disk to disk backup device shall be a purpose built backup appliance and shall be certified to work with at-least 3 Backup application vendor ISV like HPE Zerto, Veeam and Commvault etc.	

65. **C14 - Spine Switch**

Sl.	Category	Technical Requirements - Spine Switch	Compliance Yes/ No
65.1	General	The core/spines layer should be able to provide active-active redundancy so that in event of failure of a single core/ spine switch the packet forwarding between hosts should not be interrupted. All the core/ spine switches should be from same OEM.	
65.2		The Switch should have redundant hot-swappable power supplies and redundant hot swappable fans. Single PS or fan failure should not impact the functioning of the switch.	
65.3		Switch should be based on industry leading standards based Virtual output queuing architecture backed with minimum 8GB of VOQ packet buffer.	
65.4		Switch should support the complete STACK of IP V4 and IP V6 services.	
65.5		Switch should support non-blocking, wire speed performance	
65.6		Switch should have the following interfaces: Should have 96x100G QSFP28 ports populated with 36x 100G-BiDi/SDWM (duplex MM Fiber LC), 36x 100G-SR4, 12x 40G-BiDi/Univ (Duplex MM Fiber LC),12x 40G-SR4 transceivers. Should be capable to support 10G, 25G, 40G, 100G connectivity. Switch hardware, Optics, OS and TAC support should be from the same OEM.	

Sl.	Category	Technical Requirements - Spine Switch	Compliance Yes/ No
65.7		Switch should support different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/ Link Aggregation Group (LAG) etc.	
65.8		The switch should support 256K IPv4 routes, 256K IPv6 routes from day-1.	
65.9		Switch should support Graceful Restart for ISIS, OSPFv2 and v3, BGP etc.	
65.10		Switch should support minimum 20K ACL entries.	
65.11		The switch should support maintenance mode to gracefully divert traffic away from the switch during maintenance operation to minimize traffic interruption in the fabric.	
65.12		The switch should support hardware-based load balancing at wire speed using LACP and multi chassis ether-channel/LAG. Min 128-Way ECMP support.	
65.13		Switch should support total aggregate minimum 9.6Tbps of switching capacity.	
65.14		The switch should support ISIS (v4 & v6), OSPF, OSPFv3, BGP for both IPv4 and Ipv6, multi-hop BFD, MoFRR from day-1. Should be upgradable to support MPLS L3 VPN, MPLS-EVPN, EoMPLS, Segment Routing, RSVP, LDP, TI-LFA.	
65.15		Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN.	
65.16		Switch should support VXLAN and EVPN for supporting Spine Leaf architecture to optimize the east - west traffic flow inside the data Centre. Should support EVPN based ESI Active-Active Multihoming for redundant connection to servers.	
65.17		Switch Should support OISM routed multicast with EVPN VXLAN.	
65.18		Switch should support Open Config	
65.19		Switch should support minimum 200K MAC addresses. Minimum 8GB VOQ packet buffer on day-1.	
65.20		Support for broadcast, multicast and unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
65.21		Switch should support Multicast - PIM-SM, SSM,	

Sl.	Category	Technical Requirements - Spine Switch	Compliance Yes/ No
		MSDP, anycast RP	
65.22		Switch should support methods for identifying different types of traffic for better management and resilience	
65.23		Switch should support DSCP, ECN, Strict Priority Queuing, WRR scheduling	
65.24		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
65.25		Switch should support virtual output queue based architecture to avoid head-of-line blocking backed with deep packet buffers.	
65.26		Switch should support TACACS+, RADIUS, Time based ACL, DHCP Server and relay, ARP Inspection	
65.27		Switch should support control plane protection i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
65.28		Switch should support NTP, PTP (boundary and transparent mode), SNMPv3, syslog, packet capture using Wire shark, Multiple config Files, Multiple Images, Config Roll back	
65.29		The device Operating system should have an unmodified Linux kernel	
65.30		Switch should support for predefined and custom execution of script (onboard python and bash) for device manager for automatic and scheduled system status update for monitoring and management	
65.31		Switch should support logging and searching of changes in IP route table, ARP address table and MAC address table when an entry is added or deleted from the table.	
65.32		Switch should support real time state streaming telemetry for in-depth visibility and analytics (should not be dependent on SNMP and Netflow / sflow)	
65.33		The device should support detecting microburst and streaming of congestion events in Realtime.	
65.34		The Device should support remote mirroring over L3 network with packet filtering support for application monitoring & troubleshooting purpose	
65.35		The Device should support PTP transparent and boundary clock.	

Sl.	Category	Technical Requirements - Spine Switch	Compliance Yes/ No
65.36		Switch should support RPM install and docker containers to run third party or custom applications for monitoring and management flexibility.	
65.37		All proposed switches and core router in DC, DR and Near Line DC should be from same OEM.	
65.38		All proposed switches and core router in DC, DR and Near Line DC should run same OS image and should be managed from centralized manager from the same OEM.	
65.39		The production network fabric to be designed such that server to Leaf switch physical cabling remains within the same rack while providing network level Active-active redundancy.	
65.40		The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with Realtime and historical time-series database view, traffic flow analytics, flow path identification, PSIRT & Bug visibility, configuration compliance, centralised patching & upgradation, end-point visibility and search, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change workflow management, congestion monitoring, notification through email & message, 3rd party integration. Required appliance should be provided along with N+2 HA and appliance hardware should be sized to support a scale of minimum 500 network devices from day-1.	
65.41		The device OEM should be leader in Gartner's Magic quadrant in Data Centre networking for last 5 consecutive years. The device OEM should be rated as a leader by Forrester in software defined Networking	
65.42 4		The device must be quoted with direct OEM TAC support to the end customer with 4 hour replacement SLA. (TAC support should be in the name of the end customer only and there should not be any limitation on number of service request that can be raised by the end customer)	

VERIFIED

66. **C15 -Leaf Switch**.

Sl.	Category	Technical Requirements - Leaf Switch for DC/DR DC	Compliance Yes/ No
66.1	General	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
66.2		The Switch should have redundant hot-swappable power supplies and redundant hot swappable fans. Single PS or fan failure should not impact the functioning of the switch.	
66.3		Switch should be based on industry leading standards based Virtual output queuing architecture backed with minimum 4GB of VOQ packet buffer.	
66.4		Switch should have the following interfaces:	
66.5		48 x 1G/10/25G SFP28 native ports (populated with 10/25G dual rate multimode transceiver not requiring any attenuator to connect other end over 10G SR)	
66.6		8 x 100GbE QSFP ports (populated with 4x100G-BiDi/SWDM (duplex MM fiber LC), 4x100G-SR4)	
66.7		Switch should support 25G SR optics without the use of DAC cables. Switch hardware, Optics, OS and TAC support should be from the same OEM.	
66.8		The switch should support 256K IPv4 routes, 256K IPv6 routes from day-1	
66.9		Switch should support minimum 20K ACL entries.	
66.10		The switch should support graceful restart operation for ISIS, OSPFv2 and v3, BGP	
66.11		The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether-channel/LAG. Min 128-Way ECMP support.	
66.12		Switch should support minimum 2 Tbps of switching capacity	
66.13		The switch should support ISIS (v4 & v6), OSPF, OSPFv3, BGP for both IPv4 and Ipv6, multi-hop BFD, MoFRR from day-1. Should be upgradable to support MPLS L3 VPN, MPLS-EVPN, EoMPLS, Segment Routing, RSVP, LDP, TI-LFA.	
66.14		Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN	
66.15		Switch should support VXLAN and EVPN for supporting Spine Leaf architecture to optimize the east - west traffic flow inside the data Centre. Should support EVPN based ESI Active-Active Multihoming for redundant connection to servers.	

Sl.	Category	Technical Requirements - Leaf Switch for DC/DR DC	Compliance Yes/ No
66.16		Switch Should support OISM routed multicast with EVPN VXLAN.	
66.17		Switch should support Open config	
66.18		Switch should support minimum 200,000 no. of MAC addresses and 20K ACLs	
66.19		Support for broadcast, multicast and unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
66.20		Switch should support Multicast - PIM-SM, SSM, MSDP, anycast RP	
66.21		Switch should support methods for identifying different types of traffic for better management and resilience	
66.22		Switch should support DSCP, ECN, Strict Priority Queuing, WRR scheduling	
66.23		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
66.24		Switch should support virtual output queue based architecture to avoid head-of-line blocking backed with deep packet buffers.	
66.25		Switch should support TACACS+, RADIUS, Time based ACL, DHCP Server and relay, ARP Inspection	
66.26		Switch should support control plane protection i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
66.27		Switch should support NTP, PTP (boundary and transparent mode), SNMPv3, syslog, packet capture using Wire shark	
66.28		The device Operating system should have an unmodified Linux kernel	
66.29		Switch should support for predefined and custom execution of script (onboard python and bash) for device manager for automatic and scheduled system status update for monitoring and management	
66.30		Switch should support logging and searching of changes in IP route table, ARP address table and MAC address table when an entry is added or deleted from the table.	
66.31		Switch should support real time state streaming telemetry for in-depth visibility and analytics (should not be dependent on SNMP and Netflow / sflow)	

Sl.	Category	Technical Requirements - Leaf Switch for DC/DR DC	Compliance Yes/ No
66.32		The device should support detecting microburst and streaming of congestion events in Realtime.	
66.33		The Device should support remote mirroring over L3 network with packet filtering support for application monitoring & troubleshooting purpose	
66.34		The Device should support PTP transparent and boundary clock.	
66.35		Switch should support RPM install and docker containers to run third party or custom applications for monitoring and management flexibility.	
66.36		All proposed switches and core router in DC, DR and Near Line DC should be from same OEM.	
66.37		All proposed switches and core router in DC, DR and Near Line DC should run same OS image and should be managed from centralized manager from the same OEM.	
66.38		The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with Realtime and historical time-series database view, traffic flow analytics, flow path identification, PSIRT & Bug visibility, configuration compliance, centralised patching & upgradation, end-point visibility and search, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change workflow management, congestion monitoring, notification through email & message, 3rd party integration. Required appliance should be provided along with N+2 HA and appliance hardware should be sized to support a scale of minimum 500 network devices from day-1.	
66.39		The production network fabric to be designed such that server to Leaf switch physical cabling remains within the same rack while providing network level Active-active redundancy.	
66.40		The device OEM should be leader in Gartner's Magic quadrant in Data Centre networking for last 5 consecutive years. The device OEM should be rated as a leader by Forrester in software defined Networking	

67. C16- OOB Mgmt. Switch/ WAN Switch

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
67.1	General	Device should have at least 48 nos. of 1G base-T ports and 6 nos of 1/10/25G native SFP28 ports. Should be populated with 6 nos. of 10/25G dual rate multimode transceiver not requiring any attenuator to connect other end over 10G SR	
67.2		The switch should support Dual hot-swappable power supplies and N+1 hot swappable fans	
67.3		Switch should have console port and OOB management port	
67.4		Shall have switching capacity of 200 Gbps or higher	
67.5		Shall have up to 150 million pps switching throughput or higher	
67.6		The Switch should support minimum 96K MAC address	
67.7		The switch should support VLAN and tagging and support the IEEE 802.1Q standard and 4K VLAN	
67.8		The switch should support Rapid Per-VLAN Spanning Tree (RPVST+)	
67.9		The switch should support ECMP 64-way	
67.10		The Switch should support MLAG/MC-LAG HA mechanism	
67.11		The switch should support Virtual Router Redundancy Protocol (VRRP v4 and v6)	
67.12		The switch should support IEEE 802.3ad Link Aggregation Protocol (LACP)	
67.13		The switch should support IEEE 802.1s Multiple Spanning Tree	
67.14		The switch should support DHCP relay and DHCP server function	
67.15		The switch should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
67.16		The switch should support Policy-based routing	
67.17		The switch should support Border Gateway Protocol (BGP), ISIS (v4 and v6) and OSPF.	
67.18		The switch shall support up to 128k IPv4 LPM routes.	
67.19		The should support industry leading open IETF standard VXLAN + EVPN for next generation of network virtualization and SDN capability.	
67.20		The switch should support Bidirectional	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
		Forwarding Detection (BFD)	
67.21		Safety and Emission standards including EN 60950 or IEC 60950 or VCCI or FCC	
67.22		The device OEM should be leader in Gartner's Magic quadrant in Data Centre networking for last 5 consecutive years. The device OEM should be rated as a leader by Forrester in software defined Networking	
67.23		The device must be quoted with direct OEM TAC support to the end customer with 4 hour replacement SLA. (TAC support should be in the name of the end customer only and there should not be any limitation on number of service request that can be raised by the end customer)	
67.24		The switch should support IP multicast routing including PIM sparse and PIM-SSM to route IP multicast traffic	
67.25		The switch should support RADIUS and TACACS+ with role based access control	
67.26		The switch should support Secure shell, SFTP, SCP	
67.27		The switch should support Secure management access to deliver secure encryption of all access methods (CLI and MIB) through SSHv2, SNMPv3	
67.28		The switch should support Role based access control	
67.29		The switch should provide filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number	
67.30		The switch should support rate limiting / policing / shaping	
67.31		The Switch should support ACL based classification.	
67.32		Operating temperature of -5°C to 40°C	
67.33		Switch should support Min 7K ACL entries	
67.34		The switch should support mirroring to a remote device (over L3 network) with filtering support	
67.35		The switch should support Remote monitoring, SNMPv3 and IPFIX	
67.36		The switch should support Jumbo frames	
67.37		The switch should support RADIUS, TACACS+.	
67.38		Switch should support IPFIX.	
67.39		The switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
67.40		The switch should support Multiple configuration	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
		files, config sessions and rollback	
67.41		The switch should have Out-of-band Ethernet management port	
67.42		The switch should support BFD	
67.43		The switch support Open config	
67.44		The device Operating system should have an unmodified Linux kernel	
67.45		Switch should support for predefined and custom execution of script for automatic and scheduled system status update for monitoring and management	
67.46		Switch should support tracking of changes in IP route table, ARP address table and MAC address table when an entry is added or deleted from the table for logging or troubleshooting	
67.47		Switch should support real time state streaming telemetry for in-depth visibility and analytics (should not be dependent on SNMP and Netflow / sflow)	
67.48		The device should support detecting microburst.	
67.49		The Device should support remote mirroring over L3 network with packet filtering support for application monitoring & troubleshooting purpose	
67.50		The Device should support PTP transparent and boundary clock.	
67.51		Switch should support RPM install and docker containers to run third party or custom applications for monitoring and management flexibility.	
67.52		All proposed switches and core router in DC, DR and Near Line DC should be from same OEM.	
67.53		All proposed switches and core router in DC, DR and Near Line DC should run same OS image and should be managed from centralized manager from the same OEM.	
67.54		The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with real time and historical time-series database view, traffic flow analytics, flow path identification, PSIRT & Bug visibility, configuration compliance, centralised patching & upgradation, end-point visibility and search, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
		workflow management, congestion monitoring, notification through email & msg, 3rd party integration. Required appliance should be provided along with N+2 HA and appliance hardware should be sized to support a scale of minimum 500 network devices from day-1.	
67.55		The OOB network fabric to be designed such that server to OOB switch physical cabling remains within the same rack.	

68. **C17 - Core Router**

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
68.1	General	Router should have 12 nos. or more 1G SFP ports, 24 nos of 10/25G SFP28 ports and minimum 6 x 100G QSFP28 ports. Should be populated with 4x 1G-T, 4x 1G-SX, 4x 1G-LX, 8x 10G-SR, 8x 10G-LR, 8x 25G-LR, 4x 40G-SRBD/Univ (duplex MM fiber LC).	
68.2		The Router should support Dual hot-swappable power supplies.	
68.3		Router should have console port and OOB management port	
68.4		Shall have throughput of 1.2 Tbps or higher	
68.5		Shall have up to 600 million pps switching throughput or higher	
68.6		Router should be based on industry leading standards based Virtual output queuing architecture backed with minimum 2GB of VOQ packet buffer.	
68.7		The Router should support Rapid Per-VLAN Spanning Tree (RPVST+) and MST	
68.8		The Router should support ECMP	
68.9		The Router should support Virtual Router Redundancy Protocol (VRRP v4 and v6)	
68.10		The Router should support IEEE 802.3 and Link Aggregation Protocol (LACP)	
68.11		The Router should support DHCP relay and DHCP server function	
68.12		The Router should support OSPFv2 for IPv4 routing and OSPFv3 for IPv6 routing	
68.13		The Router should support Policy-based routing	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
68.14		The Router should support Border Gateway Protocol (BGP), ISIS (v4 and v6) and OSPF.	
68.15		The Router shall support 1 Million IPv4 LPM routes	
68.16		The Router should support industry leading open IETF standard VXLAN + EVPN for next generation of network virtualization and SDN capability.	
68.17		The router should support RPKI, BGP monitoring protocol, BGP-PIC, graceful restart for ISIS & OSPF & BGP, multihop BFD, URPF, IP unnumbered for ISIS & OSPF & BGP from day-1.	
68.18		The router should support MPLS, MPLS L3 VPN, 6PE/6VPE, LDP, RSVP, TI-LFA, ldp-pseudowire, MPLS-EVPN from day-1	
68.19		The Router should support Bidirectional Forwarding Detection (BFD)	
68.20		The Router should support IP multicast routing including PIM sparse and PIM-SSM to route IP multicast traffic	
68.21		The Router should support RADIUS and TACACS+ with role based access control	
68.22		Router should support Industry standard Virtual Output Queing Architecture with minimum 2 Gb of buffer.	
68.23		The Router should support Secure shell, SFTP, SCP	
68.24		The Router should support Secure management access to deliver secure encryption of all access methods (CLI and MIB) through SSHv2, SNMPv3	
68.25		The Router should support Role based access control	
68.26		The Router should provide filtering based on source/ destination IP address/ subnet and source/ destination TCP/ UDP port number	
68.27		The Router should support rate limiting/ policing/ shaping	
68.28		The Router should support ACL based classification	
68.29		The Router should support mirroring to a remote device over L3 with filtering support	
68.30		The Router should support Remote monitoring RMON/SNMPv3 and sFlow.	
68.31		The Router should support Jumbo frames	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
68.32		The Router should support RADIUS, TACACS+.	
68.33		Router should support IPFIX	
68.34		The Router should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
68.35		The Router should support Multiple configuration files, config sessions and rollback	
68.36		The Router should have Out-of-band Ethernet management port.	
68.37		The Router should support BFD	
68.38		The Router support Openconfig	
68.39		The Router Operating system should have an unmodified linux kernel	
68.40		Router should support for predefined and custom execution of script (onboard python and bash)	
68.41		Router should support tracking of changes in IP route table and ARP address table when an entry is added or deleted from the table for logging or troubleshooting	
68.42		Router should support real time state streaming telemetry for in-depth visibility and analytics (should not be dependent on SNMP and Netflow/ sflow)	
68.43		The Router should support detecting microburst and streaming of congestion events in Real-time.	
68.44		The Router should support remote mirroring over L3 network with packet filtering support for application monitoring & troubleshooting purpose	
68.45		The Router should support PTP transparent and boundary clock.	
68.46		Router should support RPM install and docker containers to run third party or custom applications for monitoring and management flexibility.	
68.47		All proposed switches and core router in DC, DR and Near Line DC should be from same OEM.	
68.48		All proposed switches and core router in DC, DR and Near Line DC should run same OS image and should be managed from centralized manager from the same OEM.	
68.49		The device should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with real time and historical time-series database view, traffic flow analytics, flow path	

Sl.	Category	Technical Requirements - OOB mgmt. Switch/ WAN Switch	Compliance Yes/ No
		identification, PSIRT & Bug visibility, configuration compliance, centralised patching & upgradation, end-point visibility and search, Zero touch provisioning, resource utilization monitoring, event notification, auto topology view, Change workflow management, congestion monitoring, notification through email & msg, 3rd party integration. Required appliance should be provided along with N+2 HA and appliance hardware should be sized to support a scale of minimum 500 network devices from day-1.	
68.50		Operating temperature of -5°C to 40°C	
68.51		Safety and Emission standards including EN 60950 or IEC 60950 or VCCI or FCC	
68.52		The device OEM should be leader in Gartner's Magic quadrant in Data Centre networking for last 5 consecutive years. The device OEM should be rated as a leader by Forrester in software defined Networking	
68.53		The device must be quoted with direct OEM TAC support to the end customer with 4-hour replacement SLA. (TAC support should be in the name of the end customer only and there should not be any limitation on number of service request that can be raised by the end customer)	

69. **C18- Virtual Server LB**

Sl.	Category	Load Balancer	Compliance Yes/ No
69.1	Virtual Server LB	Must be a virtual appliance which supports Multitenancy and Virtual Contexts, should be supported on Bare-metal, leading Hypervisors of ESXi and KVM. Should integrate with GSLB and Enterprise SIEM as provided part of project	
69.2		The solution should support Layer 7 throughput of upto aggregated 10 Gbps or higher and scalable upto 20 Gbps with additional license and allows unlimited instances without exceeding licensed aggregated throughput at any given point in time	

Sl.	Category	Load Balancer	Compliance Yes/ No
69.3		Should support minimum 800,000 Layer 7 requests per second on day 1 and scalable upto 1.5 million with additional license	
69.4		System must support 5K SSL TPS for 2K bit key and on demand upgradable upto 10K TPS for 2K bit key with 6 Gbps of bulk encryption or higher	
69.5		The solution should have inbuilt multi-tenancy and should support auto-discovery, Integration and Orchestration of the underlying infrastructure on which it has been deployed.	
69.6		The proposed solution should have a Central Management station which support Auto-Discovery, Integration and Orchestration of the underlying cloud on which it has been deployed	
69.7		The solution should support auto scale out and scale in functionality so that when traffic load increases, required load balancer instances are added or deleted on demand.	
69.8		The solution should support application monitoring, end-to-end round trip times with latencies, "network DVR" like record and review capabilities, searchable traffic logs, security insights, log insights, client insights etc.	
69.9		The solution should provide an application health score which takes into account application performance, resource utilization, anomaly and security penalties.	
69.10		The solution should support IP and cookie persistence and should support SSL offload.	
69.11		The solution should be capable to provide L4 load balancing to a service mesh environment comprising of Istio gateway.	
69.12		The solution should provide full automation with REST APIs to support faster application rollout in blue/green and canary deployments.	
69.13		The solution should support various load balancing algorithms such as least connections, round-robin, hash, weighted round robin and response time.	
69.14		The solution should offer automation of deployment, configuration and lifecycle management of the data Plane entities in environments such as VMware, Kubernetes, Open shift etc	
69.15		The solution should support Global Server Load Balancing and cross-cluster service discovery for external applications using inbuilt DNS.	

Sl.	Category	Load Balancer	Compliance Yes/ No
69.16		The solution must support various Security features at the Ingress to the Kubernetes Cluster - WAF, Application Rate Limiting, L3/L4/L7 Firewall Rules, SSL/TLS Termination, Client Authentication etc	
69.17		The solution must provide native DNS and IPAM capabilities as well as support/integration with popular DNS & IPAM providers like Infoblox, Route53, Azure IPAM/DNS etc.	
69.18		The solution should be an Integrated Solution offering L4-L7 LB, WAF, GSLB and Analytics for K8s Ingress	
69.19		The product should offer integrated solution for Application-Layer security through a Web Application Firewall located at or after SSL/TLS termination of the traffic flows.	
69.20		The product should offer an integrated and cloud-native solution for Global Server Load Balancing (GSLB) supporting multi-cluster application deployments.	
69.21		The Product should offer in-depth analytics for the North-South traffic flows including latency/end-to-end timing analysis of flows, application performance monitoring, client and log analytics and dynamic health scoring.	

70. **C19 - Software Defined WAN**

Sl.	Category	Technical Requirement of SD-WAN	Compliance Yes/ No
70.1	Form factor	The proposed branch solution should be available in both pre-packaged physical appliance and software virtual form factor.	
70.2	Central orchestrator	The solution should compromise of a centralized orchestrator capable of configuration and monitoring of multiple WAN Edge devices in the branches, data-centres and remote locations. Solution should also compromise of a high-performance branch Customer Premises Equipment (CPE) or Virtual CPE devices which can replace traditional WAN routers or co-exist with traditional WAN routers. These branches are to be managed from the centralized orchestrator. The centralized orchestrator should also provide for an option of remote diagnostics to validate reachability of both	

Sl.	Category	Technical Requirement of SD-WAN	Compliance Yes/ No
		WAN and LAN sides, packet captures ARP tables, route tables etc. The proposed solution should provide an option of using the Orchestrator (Management and Provisioning Platform) from a public cloud and it should also have the capability to be deployed on-premises.	
70.3	Bandwidth aggregation	The proposed hub/CPE devices should be able to aggregate the bandwidth across multiple links and should have zero-IT touch deployment capabilities.	
70.4	Link steering	The solution should provide for sub-second per-packet link steering based on the measured performance metric, application requirements, business priority of the application and link cost The solution should provide for on-demand link remediation in the event of packet loss, increase in latency and jitter	
70.5	Transport agnostic	The proposed solution should be an enterprise grade WAN solution and should be completely transport independent. And, should support multiple technologies like MPLS, Internet, P2P Links, 3G/4G/LTE.	
70.6	Application awareness	The solution should be able to detect, classify and control various applications running over WAN. The solution should provide historical and real time link usage and performance of applications. The solution should provide for application usage related data over time and should provide an option to filter it down to things like Source Devices/IPs, destinations etc.	
70.7	Multi-hypervisor support	The branch device should be capable of running/supported over major hypervisors like VMware and KVM	
70.8	VPN Tunnels	The solution should enable creation of full mesh, partial mesh and hub-n-spoke VPN tunnels including dynamic branch to branch tunnels with a single click.	
70.9	Link fail-over	The solution should be capable of detecting WAN failures and dynamically steering the traffic to available WAN links in a sub-second manner.	

Sl.	Category	Technical Requirement of SD-WAN	Compliance Yes/ No
70.10	Quality of Service (QoS)	The solution must be able to define classes of application traffic and apply Quality-of-Service policies to each class. The solution must be able to apply QoS policies to all traffic seen in the network, including both optimized and non- optimized traffic flows, including TCP, UDP, and other non-TCP traffic types.	
70.11		The solution must be able to apply inbound QOS by TCP/UDP rate limiting low priority traffic. QoS policies should be centrally defined and can be applied to classes of applications and individual applications	
70.12	Encryption	The encryption scheme used by SD-WAN solution should be FIPS 140-2 compliant. The solution should provide 128-bit AES or 256-bit AES encryption on the VPN. The branch device should have an inbuilt firewall for providing Layer 4 policies and the branch device should also be capable of running 3rd part firewall VNFs and provide service chaining for the same.	
70.13	Bandwidth throughput	WAN bandwidth of 8 Mbps at ROBO site and 40 Mbps at Central Data Centre site	
70.13	Single-pane-of-glass monitoring	Should provide Enterprise level unified Dashboard 'Single-pane-of-glass-monitoring and management' from central site for all ICG DC/ DR/ ROBO sites. Should support single unified policy across all sites	

71. **<u>C20 - SAN Switch</u>**.

Sl.	Technical Specifications – SAN Switch	Compliance Yes/ No
71.1	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 48 Ports scalable to 96 ports.	
71.2	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.	
71.3	Should deliver 16 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports or more in an energy-efficient, optimized 1U form factor.	
71.4	Should protect existing device investments with auto-sensing 4,	

Sl.	Technical Specifications – SAN Switch	Compliance Yes/ No
	8, 16 and 32 Gbps capabilities.	
71.5	The switch shall support different port types such as FL Port, F Port, E Port	
71.6	The switch should be rack mountable.	
71.7	Offered Switch shall be provided with redundant FAN and shall have option for redundant power supply.	
71.8	Non-disruptive Microcode/ firmware / Software Upgrades and hot code activation.	
71.9	The switch shall provide Aggregate bandwidth of minimum of 1536 Gbit/sec end to end in full duplex mode.	
71.10	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.	
71.11	SAN switch shall support to restrict data flow from less critical hosts at present bandwidths.	
71.12	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.	
71.13	The switch shall be able to support ISL trunk up to 128 Gbit/sec or more between a pair of switches for optimal bandwidth utilization and load balancing.	
71.14	SAN switch shall support to isolate the high bandwidth data flows traffic to specific ISLs.	
71.15	Switch shall support to measure the top bandwidth-consuming traffic in real time for a specific physical or virtual device, or end to end across the fabric.	
71.16	Switch shall have support for web based management and should also support CLI.	
71.17	The switch shall support advanced zoning and ACL to simplify administration and significantly increase control over data access.	
71.18	SAN switch shall have support to configure the switches with alerts based on threshold values for temperature, fan status, Power supply status, port status.	
71.19	Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute),	

Sl.	Technical Specifications – SAN Switch	Compliance Yes/ No
	port mirroring (SPAN port).	
71.20	The switch should have USB port for firmware download, support save, and configuration upload/download.	
71.21	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.	

72. **C21 - Passive Cabling**. As per tier-III data centre standards

73. **C22 - Enterprise Mgmt. Solution Suite**.

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.1	Generic / Functional	The EMS shall support single pane/ dashboard for the purposes of the NOC with real time monitoring & visibility across multiple areas of DC environment for monitoring. The EMS solution shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components.	
73.2	Generic / Functional	The EMS shall be capable of providing early warning signals to the NOC on the performance issues, and future infrastructure capacity augmentation. The alarms should contain meaningful message text, instruction text, operator/ automatic actions/ linked graphs, duplicate message suppression.	
73.3	Generic / Functional	The EMS solution shall help the NOC to quickly triage the root cause for a network problem or service availability and provide actionable information to the respective teams for a quick resolution to the problem before end users get impacted.	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.4	Generic / Functional	The alerting mechanism should be configurable to suppress events at the agent or managed node level itself and be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.	
73.5	Generic / Functional	The EMS solution shall offer service driven operations management of the IT environment to manage distributed, heterogeneous systems from a single management station. The solution shall provide comprehensive and end-to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure.	
73.6	Generic / Functional	The EMS solution will also let the NOC team monitor and request reports for SLA requirements as agreed upon for various services both on availability & performance.	
73.7	Generic / Functional	The EMS solution should be able to monitor and provide availability reports for assets both within and outside the datacentre. The EMS solution will allow to associate an asset with a consuming service so that it can be appointed a business value and its impact and utilization in the environment can be understood by the business.	
73.8	Generic/ Functional	The EMS solution will provide comprehensive server monitoring capabilities to understand the processes & services running on a machine and resource utilization impact's performance such as a Database service, web server, application server etc.	
73.9	Generic/ Functional	The EMS solution should include asset management capabilities to monitor the lifecycle for all assets, both hardware and software, in the environment. It shall also	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		allow the team to generate detailed reports for effective management such as reports on asset utilization, end of service, maintenance lifecycle etc.	
73.10	Generic/ Functional	The solution should provide seamless integration between discovery, monitoring and service desk tools which will help in automated ticket logging in service desk for all the critical events occurring in centralized monitoring console and to keep an updated CMDB. It shall also provide flexibility of logging, viewing, updating and closing incident manually via web interface.	
73.11	Generic/ Functional	The proposed helpdesk system shall support ITIL processes like request management, incident, problem management, knowledge, SLM, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	
73.12	Generic/ Functional	The EMS solution shall be able to accurately measure the KPIs/ SLAs agreed upon by and report them on pre-communicated intervals to the key stakeholders for analysis. The SLA & KPI details should be obtained directly from application & platform owners and agreed upon by team as well. For continued improvement, these SLAs/ KPIs might need to be updated from time to time to reflect the maturity of the environment after agreement with team.	
73.13	Generic / Functional	MSI shall use Industry standard EMS tools recognized by analysts (like Gartner, Forrester etc.) to report desired SLA's for availability & performance of Various IT Components including Networks, Systems and OS.	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.14	Generic / Functional	The EMS solution tools must be open to integration not only among themselves but also with other technologies being utilized such as the Single pane view dashboard for the NOC & other SLA & Reporting technologies being utilized by different applications. EMS solution will capture valuable data which will prove useful to other solutions such as the GIS solution for example to populate device data on visualization screens. Similarly, data integration will also have to be considered with the ERP HR modules to get approval flows and access levels of various resources for an ITSM request catalogue.	
73.15	Generic / Functional	To ensure EMS doesn't introduce any unsolicited security loopholes and concerns, only SNMP v3 compliant devices must be integrated with the EMS systems and the MSI should ensure that non-standard ports and non-standard community strings are always used where possible.	
73.16	Generic / Functional	All EMS tools and applications must utilize non-default ports and all communications must be secured via SSL.	
73.17	Service monitoring & reporting	The solution shall include a service management system which shall provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.	
73.18	Service monitoring & reporting	The MSI is obliged to regularly monitor the SLAs and KPIs as set out in "Service Level Management" documents agreed upon. In case of degradation in actual performance, this shall be escalated by the Supplier to the right level in the organization and follow up until resolution as per agreed SLAs. The Supplier shall	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		keep informed about such escalations at mutually agreed time intervals and maintain a log of all escalations and messages or actions related to the escalations.	
73.19	Service monitoring & reporting	The solution shall provide an outage summary that gives a high-level health indication for each service as well as the details and root cause of any outage.	
73.20	Service monitoring & reporting	The solution shall manage IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements.	
73.21	Service monitoring & reporting	The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).	
73.22	Service monitoring & reporting	SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.	
73.23	Service monitoring & reporting	The solution shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an applicable SLA shall be available.	
73.24	Service monitoring & reporting	The solution shall provide reports which include service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.25	Service monitoring & reporting	The solution shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service-related metrics with capabilities for customization of the report presentation.	
73.26	Service monitoring & reporting	The solution shall provide for customizing service policies as per service owner definitions like Service Condition High/ Low Sensitivity, service SLAs, violation conditions etc. shall be provided out of the box.	
73.27	System Monitoring	The solution shall present a centralized management console & dashboard across both physical and virtual systems.	
73.28	System Monitoring	The solution shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored if needed.	
73.29	System Monitoring	It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.	
73.30	System Monitoring	It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.	
73.31	System Monitoring	The solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.	
73.32	System Monitoring	The tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services can be automatically re-started	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.33	System Monitoring	The tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable them to take applicable actions.	
73.34	System Monitoring	The performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.	
73.35	System Monitoring	It shall be able to automate monitoring, data collection and analysis of performance from single point.	
73.36	System Monitoring	It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) or application owners to quickly trace and resolve performance-related bottlenecks.	
73.37	System Monitoring	The system shall provide Performance Management and Reporting- Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines.	
73.38	System Monitoring	The solution should be made available in a High Availability setup & should be able to stably support at least 800 systems in the Datacentres both Physical and Virtual.	
73.39	Network monitoring	The EMS solution shall be capable of supporting multiple types of discovery like IP range discovery – including built-in support for IPv6 and discovery whenever new devices are added with capability to	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		exclude specific devices.	
73.40	Network monitoring	The solution shall support exclusion of specific IP addresses or IP address ranges as per discovery requirements.	
73.41	Network monitoring	The solution shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.	
73.42	Network monitoring	The solution shall be able to identify and model the ICT asset and its properties in the solution when discovered.	
73.43	Network monitoring	The solution shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason as applicable.	
73.44	Network monitoring	The solution shall provide out of the box root cause analysis for any observed fault or outage.	
73.45	Network monitoring	The solution shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.	
73.46	Network monitoring	The solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.	
73.47	Network monitoring	The solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.	
73.48	Network monitoring	The solution shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.	
73.49	Network monitoring	The solution shall have all the capabilities of a Network Management System which shall provide Real time network	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		monitoring and Measurement offer end-to-end network performance & availability to define service levels and further improve upon them."	
73.50	Network monitoring	The solution shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.	
73.51	Network monitoring	The solution shall have the capability to configure different polling speeds for different devices in the managed infrastructure.	
73.52	Network monitoring	The solution shall provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The solution shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The solution shall also intelligently determine which ports are operationally dormant	
73.53	Network monitoring	The Network Performance Management console shall provide a consistent report generation interface from a single central console.	
73.54	Network monitoring	This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources	
73.55	Network monitoring	The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.	
73.56	Network monitoring	The proposed system shall provide an integrated performance view for all the managed systems and networks along	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		with the various threshold violations alarms in them.	
73.57	Network monitoring	The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.	
73.58	Network monitoring	The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.	
73.59	Network monitoring	The solution should be made available in a High Availability setup & should be able to stably support at least 2200 network devices & switches (1U/2U/IE/chassis-based) in the environment.	
73.60	Application monitoring	The solution shall proactively monitor all user transactions for any web application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.(Application Monitoring)	
73.61	Capacity Monitoring	The proposed solution should provide visibility into the entire IT infrastructure—physical, virtual, and cloud	
73.62	Capacity Monitoring	The proposed solution should provide Service views, forecasting, modelling and reservation capabilities in order to provide the insight for future resource needs and the ability to control the timing and cost of new capital and operating expenditures	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.63	Capacity Monitoring	The proposed solution should have the ability to allocate and schedule needed IT infrastructure resources for day-one use so that the IT has a view of both realized and utilized IT resources and thereby IT can plan for onboarding or infrastructure acquisitions	
73.64	Capacity Monitoring	The proposed solution should have the ability to forecast and model changes in service demand so that IT can easily adjust the infrastructure resources based on peak, cyclic, or growth in demand	
73.65	Capacity Monitoring	The proposed solution should be able to optimize resources with complete visibility for on-premises and public infrastructure services.	
73.66	Capacity Monitoring	The proposed solution must have support for all the available latest clouds, so that IT can have insight into resource utilization and needs regardless of where or how workloads are run	
73.67	Capacity Monitoring	The proposed solution should have the ability to identify the cost of service so that IT can provide lines of business with the financial information they need for creating competitive services	
73.68	Capacity Monitoring	The proposed solution should be able to gather data for all of the infrastructure resources that are important for application and service performance	
73.69	Capacity Monitoring	The proposed solution must provide IT the capability to deploy applications on time by reserving IT resources for new applications and services when needed	
73.70	Capacity Monitoring	The proposed solution must provide IT the capability to deploy applications on time by reserving IT resources for new applications and services when needed	
73.71	Capacity Monitoring	The proposed solution must provide IT the capability to optimize costs with the	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		insight to invest in new physical, virtual, or cloud IT resources only as needed	
73.72	Capacity Monitoring	The proposed solution must provide IT the capability to gain visibility across the enterprise, including physical, virtual, private and public cloud, and Hadoop infrastructure resources	
73.73	Application monitoring	The solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.	
73.74	Application monitoring	The solution shall be able to obtain request response times based on different call parameters.	
73.75	Application monitoring	The solution shall be able to correlate Application changes (code and configuration files) with change in Application performance.	
73.76	Application monitoring	The solution shall be able to limit access to data by user roles e.g. Data for an application should be visible only to the application's owners	
73.77	Application monitoring	The solution shall give visibility into end user experience for various transactions without the need to install agents on end user desktops.	
73.78	Application monitoring	The solution shall act as a passive listener on the network thus inducing zero overhead on the network and application layer particularly during peak loads.	
73.79	Application monitoring	The solution shall be able to detect user impacting defects and anomalies and reports them in real-time such as in case of a Slow Response Time, Partial response, Missing component within transaction, HTTP error codes, web application errors etc.	
73.80	Application monitoring	The solution shall be able to provide trend analysis reports and compare the user experience over time by identifying	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		transactions whose performance or count has deteriorated over time.	
73.81	Application monitoring	The solution should be made available in a High Availability setup & should be able to stably support at least 12 applications with possibility for adding more apps in the future based on the requirements.	
73.82	Asset and Patch Management	The system management solution should include a patch management tool which will manage the entire lifecycle of patches, hot-fixes, updates and service packs from automatic discovery, download and collection, thorough testing, conflict analysis, and vulnerability assessment, to policy-based targeting and deployment and ongoing management to ensure that patches stay applied as prescribed by policy.	
73.83	Asset and Patch Management	The solution shall automatically sense and apply patches (install, uninstall, repair, self-healing) on the clients, eliminating the need to create lists and administrator jobs (no admin intervention). If a certain patch is deleted or un-installed from any desktop by the user, it should automatically be repaired/ re-installed without the intervention of the Administrator to reduce helpdesk calls.	
73.84	Asset and Patch Management	Solution should enable the administrator to generate real time patch compliance reports based on created policies, reports on failed patch deployments and systems pending restart etc. for streamlining the process.	
73.85	Asset and Patch Management	The solution shall include Service Asset and Configuration Management capabilities to fulfil the following requirements:	
73.86		Develop, Implement and Maintain Asset Management Processes and Tools	

Sl.	**Category**	**C22 - Enterprise and Network Management System for IT Operations & Monitoring**	**Compliance Yes/ No**
73.87		Maintain Asset records relating to the Services in online asset inventory, Configuration and management system (CMDB).	
73.88		Provide, develop, implement and maintain online Asset and Configuration	
73.89		Management tools that support automatic discovery and facilitate effective deployment and re-use of Assets and provide a common view of information.	
73.90		Develop, implement and maintain forms, processes and Tools related to Asset and Configuration Management and compliance to support tracking Changes across multi-provider Environment (add/ modify/ delete).	
73.91		Establish, update, and maintain CIs in the Asset and Configuration Management database (CMDB)	
73.92		Manage every asset from requisition through retirement and the facility to track changes by maintaining history of an asset	
73.93	Asset and Patch Management	The CI level of Asset information shall include at the minimum:	
73.94		Manufacturer	
73.95		Model	
73.96		Serial number	
73.97		Asset identification number	
73.98		Asset location	
73.99		Maintenance information and history including the age of the Asset	
73.100		Ownership information (provider/ lease/ purchase)	
73.101		Warranty information	
73.102		End of Support Information	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.103		End of Life Information	
73.104		Service tag descriptions (both on CI and CI group level), including the possibility to tag which application/ usage an Asset is used for	
73.105		Inter-relationships and dependencies between Assets and applications/ Services, with necessary CI level of details to conduct Impact Assessment and analysis	
73.106		Other information as mutually agreed	
73.107	Asset and Patch Management	The solution shall support the functionality to -	
73.108		Add, modify, and delete access to appropriate fields within CMDB.	
73.109		Maintain assets and relationship, contact and escalation information to ensure Application supportability.	
73.110		Propose Hardware and Software procurement and management models and methodologies.	
73.111		Manage (full Lifecycle) and make recommendations working with DMIC representatives for lease and maintenance agreements.	
73.112		Perform monthly physical Asset audit, in accordance with the Asset Management Services, to validate that Data in the database is accurate and current and that the Information is provided as defined. Physical Asset audit shall be based on statistically significant sample size. 100% sampling is not required.	
73.113		Establish CMDB process interfaces across all associated Cross-Functional processes and IT functions.	
73.114		Align CMDB updates process with Service Introduction and Change Management removal, addition or updating of CMDB	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		data	
73.115		Manage and coordinate with Third Party and multi-partner to ensure accurate: inventory; Documentation; install/ move/ add/ change (IMAC); Refresh; and decommission across the Environment in accordance with Change and Problem Management processes.	
73.116	Asset and Patch Management	Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them	
73.117	Asset and Patch Management	Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs	
73.118	Asset and Patch Management	Ability to provide the facility to collect custom information from desktops and ability to recognize custom applications on desktops	
73.119	Asset and Patch Management	Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned	
73.120	Asset and Patch Management	Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group	
73.121	Asset and Patch Management	Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		programs/ games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc.	
73.122	Asset and Patch Management	Assets must be identified and tracked location; user/department wise.	
73.123	Asset and Patch Management	Server details must be managed in the System to ensure stakeholder management.	
73.124	Asset and Patch Management	Proactive asset manager must be enabled to notify the stakeholder when the warranty of the asset expires as this helps the asset team to proactively manage end of life assets effectively.	
73.125	Asset and Patch Management	Manage contract service levels in the system to track the End of Life Assets	
73.126	Asset and Patch Management	Vendor details must be maintained in the system to map the assets.	
73.127	Asset and Patch Management - Server	Support of Heterogeneity	
73.128		Support for all major OS and virtualization platforms	
73.129	Asset and Patch Management - Server	Built-In Rollback-Should Support comprehensive and Patch level roll-back for changes	
73.130	Asset and Patch Management - Server	Complete Automation Capabilities -- Automated provisioning for physical, virtual, and cloud-based environments	
73.131		Policy-based, Cross-Platform patch support across Windows, Linux, and Unix	
73.132		Automated packaging, promotion, and deployment of Patches	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.133	Asset and Patch Management - Server	Composite Packaging	
73.134		-Should support cross-platform and reusable packaging with built-in rollback support	
73.135	Asset and Patch Management - Server	Role Based Access Control-Should support Patch-level Control of Tasks, Objects, and Policies	
73.136	Service Desk - Discovery	Agentless Discovery-Solution should support complete agent-less discovery requiring no software to be installed on devices to be discovered.	
73.137	Service Desk - Discovery	Discovery Breadth – Simple to Complex Enterprises	
73.138		Discovery solution should do a complete discovery of IT environment across distributed, virtual and heterogeneous environment and provide a clear and visual mapping of IT infrastructure to business services.	
73.139		Should support discovery of Physical, virtual, network, application, storage and mainframe resources	
73.140	Service Desk - Discovery	Automatic Application Dependency Mapping	
73.141		Automatically map IT infrastructure to business services	
73.142		Should have at least 20,000 + application blueprints to identify DC application software.	
73.143	Service Desk - Discovery	Dynamic CMDB Integration	
73.144		Should support continuous updates of configuration & dependency data for applications	
73.145	Service Desk - Discovery	Fully Auditable Discovery Results & Diagnostics	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.146		The discovery data should be fully auditable as to where it came from and what was the method to retrieve that should support troubleshooting and diagnostics for any discovery scan failures	
73.147	Service Desk - Discovery	Reporting-Should provide OOB reports with full text search capabilities	
73.148	Service Desk - CMDB	Multiple Datasets support-The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.	
73.149	Service Desk - CMDB	Definitive Software/ Media Library -The Configuration Management should support Definitive Software and Media Library with content updates on a periodic basis.	
73.150	Service Desk - CMDB	Normalization-Normalization of data should be possible along complete definitive media library – software, hardware with standardization on attributes.	
73.151	Service Desk - CMDB	Reconciliation-Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes	
73.152	Service Desk - CMDB	Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.	
73.153		Should provide best in class integration capabilities with CMDB compliant APIs.	
73.154	Service Desk - CMDB	Unified Service Model-- Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.155		Should Provide a Service catalogue so as to establish a framework for Service definitions based on IT and business alignment	
73.156		Should Provide Service blueprints to describe functional and deployment models for the Service definitions	
73.157		Should automatically create Service models to decsribe how IT infrastructure supports business services	
73.158	Service Desk - CMDB	Single Source of Truth across Hybrid Environments-Manage services consistently across heterogeneous data Centre and cloud environments	
73.159	Service Desk - ITSM	The Solution should have the complete ITIL process flow for Incident, problem and Change, Service Desk, SLM and knowledge Management etc. compliant to ITIL V4 standards or latest.	
73.160		The solution should support capability to receive, manage and respond to issues, requests, Incidents, Problems etc. communicated within the ITSM tools.	
73.161		The solution should provision the administrator to create new or modify existing workflows.	
73.162		For integrations with other EMS/ NMS tools, various options for integration should be provided - APIs, web services, SDKs.	
73.163	Service Desk - ITSM	The solution should allow for, at the minimum, for the following capabilities:	
73.164		The flexibility of logging incidents via various means - be it manual or automatic via integration within the EMS solution.	
73.165		It should allow detailed multiple levels/tiers of categorization on the type of incident being logged.	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.166		It should provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels.	
73.167		The MSI shall recommend, document (textual and graphical as appropriate) and implement best practices for Incident Management via the solution.	
73.168		Maintain contact, escalation and notification requirements (e.g. email, phone, including Alerts) for Incidents.	
73.169	Service Desk - ITSM	The solution shall provide cross functional coordination required for incidents and major incidents such as automated integration to the Event, Problem, technical and functional change, Configuration. The solution should support Incident & problem driven change-release deployment activities	
73.170	Service Desk - ITSM	The solution should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.	
73.171		The solution should deliver service level information and alerts directly to IT Operations and Service Support consoles.	
73.172	Service Desk - ITSM	The solution shall record, document and track all Changes regarding Equipment and Software within the CMDB maintained	
73.173		The solution shall contain Audit trail of any and all Changes including authorization, type of Change and status	
73.174		The solution should manage communication, coordination, Monitoring and scheduling of Changes in computing environment with the stakeholders. It should allow Involvement of CAB and change managers to provide authorization for change requests.	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
73.175		Maintain all Configuration Data of the change management system	
73.176		Maintain Post Implementation Review for the Normal and Emergency Changes	
73.177		The solution should support Change Impact and change collision detection based on affected CIs from CMDB.	
73.178		The solution should provide for Change Calendar with periodical views for change tracking.	
73.179	Service Desk - ITSM	The solution shall provide for following Problem Management capabilities: Record, document and track all problems	
73.180		Maintain RCA and solutioning details to avoid the recurring incidents	
73.181		Ability to create change request for the problem ticket	
73.182		Auto Assignment of problem based on the category	
73.183		Ability to create knowledge from the problem	
73.184		The workflows should be able to perform notification via email to the problem managers and problem analysts	
73.185	Service Desk - ITSM	The solution shall allow for request management with following capabilities:	
73.186		Monitor the status of Service Requests including approvals and changes to delivery dates	
73.187		Maintain appropriate controls to ensure the necessary approval of requests such that only authorized individuals are able to place Service Requests.	
73.188	Service Desk - ITSM	The solution should support developing, supporting and update Knowledge Management (KMDB) to gather, analyse, store and share knowledge.	
73.189	Service Desk - ITSM	The solution should support reporting on	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		the process flow to allow management to understand how organization is performing in terms of process adherence.	
73.190	Service Desk - ITSM	The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.	
73.191		Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.	
73.192		The solution should provide for best in class integration capabilities with CMDB The solution should Provide a single shared view of services supporting Service	
73.193		Design, Transition and Operations stages of the lifecycle.	
73.194		The solution Should automatically create Service models to describe how IT infrastructure supports business services.	
73.195		Maintain vendor details when the incidents requires vendor involvement for the closure	
73.196	Service Desk - ITSM	The solution should Provide a Service catalogue so as to establish a framework for Service definitions based on IT and business alignment.	
73.197		The solution Should Provide Service blueprints to describe functional and deployment models for the Service definitions.	
73.198	Service Desk - Integration	The proposed network management system shall integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		managed asset and associate an SLA to the ticket in the helpdesk.	
73.199	Integration	SLA's violation on monitored end user response time shall open a helpdesk incident out of the box.	
73.200	Integration	Proposed Application Performance Solution shall integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.	
73.201	Integration	The proposed Fault Management Solution shall support integration with Proposed help desk or trouble ticketing system such that integration shall Associates alarms with Service Desk tickets in the following ways:	
73.202		Manually creates tickets when requested by Fault Management GUI operators	
73.203		Automatically creates tickets based on alarm type	
73.204		Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.	
73.205		Helpdesk ticket number created for associated alarm shall be visible inside Network Operation Console.	
73.206	Integration	The proposed NMS shall provide unified workflow between the fault and performance management systems including bi-directional and context sensitive navigation, such as:	
73.207		Navigate from the Topology View to At-a-Glance or Trend Reports for any asset	
73.208		Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports	
73.209		Proposed Performance Management	

Sl.	Category	C22 - Enterprise and Network Management System for IT Operations & Monitoring	Compliance Yes/ No
		system shall feed in discovery from	
73.210		Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine.	

74. **C23- DR Automation.**

Sl.	Category	DR Automation	Compliance Yes/ No
74.1	DR Automation	The solution provides centralized automated disaster recovery, site migration and non-disruptive testing capabilities to the customers.	
74.2		The solution should work in conjunction with various replication solutions including both the VM/ Hypervisor based replication and array-based replication to automate the process of migrating, recovering, testing, re-protecting and failing-back virtual machine workloads.	
74.3		The solution should act as the same site to serve as a protected site and recovery site when replication is occurring in both directions and protecting virtual machines at both sites.	
74.4		The migration of protected inventory and services from one site to the other should be controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools to which they are allocated, and the networks they can access.	
74.5		The solution should be able to Map virtual machines to appropriate resources on the failover site	
74.6		The solution should provide option to customize the shutdown of low-priority virtual machines at the failover site to get more resources or proper utilization of resource and should provide option to recover multiple sites into a single shared recovery site	
74.7		The solution should offer multiple recovery plans that can be configured to migrate individual applications and entire sites providing finer control over what virtual machines are failed over and failed back. Support the extension of recovery	

Sl.	Category	DR Automation	Compliance Yes/ No
		plans with custom scripts, control access to recovery plans with role-based access control. This also enables flexible testing schedules	
74.8		The solution should be able to initiate recovery plan execution from virtualization manager with a single click and able to support automated boot of protected virtual machines with pre-specified boot sequence	
74.9		The solution should offer:	
74.10		Application-agnostic protection eliminates the need for app-specific point solutions	
74.11		Automated orchestration of site failover and failback with a single-click reduces recovery times	
74.12		Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives	
74.13		Centralized management of recovery plans from the virtualization manager console replacing the manual runbooks	
74.14		Planned migration workflow enables disaster avoidance and data Centre mobility	
74.15		Reduce the DR footprint through hyper-converged, software defined storage	
74.16		VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage	
74.17		Support for array-based replication offers choice and options for synchronous replication with zero data loss	
74.18		Self-service, policy-based provisioning via Storage Policy Based Protection Groups, Orchestration and Automation layer automates protection""	
74.19		The solution should be able to manage and monitor execution of recovery plans from virtualization manager and support automated reconfiguration of virtual machine IP addresses at failover site. Should receive automatic alerts about possible site failure.	
74.20		The solution should be able to automate failback to original production site using original recovery plan and also able to automatically re-protect virtual machines by reversing replication to the original site	

Sl.	Category	DR Automation	Compliance Yes/ No
74.21		The solution should be able to use storage snapshot to perform recovery tests without losing replicated data and also provide multiple point-in-time recovery which will allow reversion to earlier known states	
74.22		The solution should enable the non-disruptive testing of recovery plans, using a temporary copy of the replicated data, and isolated network and storage environments in a way that does not disrupt ongoing operations at either site. This provides for the ability to test disaster recovery, disaster avoidance, or planned migrations as frequently as desired to ensure confidence in the configuration and operation of recovery plans.	
74.23		The solution should be able to store, view and export results of test and failover execution from virtualization manager and automate clean-up of testing environments after completing tests	
74.24		It should be able to manage replication directly through virtualization manager, at a granular virtual-machine level. Ensure complete replication of virtual machine data in an application-consistent state, prior to initiating migration	
74.25		The solution should be able to automate planned migrations with graceful shutdown of protected virtual machines at the original site thus ensuring zero data loss and application-consistent migrations	
74.26		The solution should provide storage-agnostic replication that supports use of low-end storage, including direct-attached storage and also provides host-based replication which will replicate only changed blocks to increase network efficiency	
74.27		The solution should provide automatic generation of history reports after the completion of workflows such as a recovery plan test and clean-up are performed in DR solution. These reports should document items such as the workflow name, execution times, successful operations, failures, and error messages which are useful for internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to HTML, XML, CSV, Microsoft Excel, Word document.	

Sl.	Category	DR Automation	Compliance Yes/ No
74.28		The solution should provide support for Stretched Storage, orchestrated cross site Virtual Machine migration and integration with Software defined network solutions	
74.29		OEM should provide direct support for L1, L2 and L3 levels 24x7x365 with unlimited incident support and 30 mins or less response time including the unlimited upgrades and updates.	
74.30		The solution should offer Layer-2 VPN allows you to extend your data Centre by allowing virtual machines to retain network connectivity across geographical boundaries.	
74.31		The solution should offer extending Layer-2 overlay across multiple sites, so that same subnet is available across these sites for configuring virtual machines.	
74.32		The solution should support reduction in Recovery Time Objective by allowing the virtual machines to retain the same IP address after migration from DC to DR, the default gateway router should be stretched across data centres, and also the firewall policies should also be applied across DC & DR.	

75. C24 –Backup Software

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
75.1	High Availability	No Single-Point-of-Failure architecture and associated components should be provided	
75.2		The solution should support VM on HA configuration	
75.3	Licensing	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.	
75.4	Application awareness	Backup software should be totally agentless but should support application aware backups for Exchange transaction logs with non-staged granular recovery of all these	

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
		applications. It should support crash consistent VM level backup for all other workloads.	
75.5	Hardware Agnostic	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.	
75.6	Granular recovery	Backup software should support file level recovery from an image level backup of Windows/ Linux guest file systems.	
75.7		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.	
75.8	VM replication	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 network addresses at the destination site.	
75.9	Unified console operation	Backup software should provide Backup and Replication capabilities in one console only.	
75.10	Encryption, WAN optimization	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.	
75.11		The proposed backup solution must support at least AES 256-bit encryption capabilities for Data-in-Rest, Data-in-Transfer support	
75.12	Tape library	Should support tape mirroring of the same job running concurrently with primary backup.	
75.13		Should allow creating tape clone facility after the backup process.	

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
7514.	Recovery verification	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its recoverability.	
75.15		Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.	
75.16	API Integration	Should provide RESTful API for integration with 3rd party Enterprise applications	
75.17	Unified management console	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.	
75.18	Replication on offline connectivity	Should support auto ROBO replication with central site on restoration of network without any manual intervention	
75.19		Recovery of ROBO sites from central backup at data Centre should be supported with zero-touch at ROBO. Take backup of ROBO sites locally and then replicate it to central location	

76. **C25- SIEM & SOAR**

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
76.1	General Requirements	The proposed solution must include Log Management, Next Gen SIEM, Security Analytics, Big Data Analytics with necessary automation capabilities from a single OEM. The solution index gigabytes of data per day on commodity hardware and provide multi-tier horizontal scalable architecture without the requirement of a HDFS file system. The solution should be built on software that can be deployed on physical or virtual infrastructure. The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices,	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		locations, applications, etc. The proposed solution must be able to collect, capture, categorize, filter, index, search event data, logs and alerts in real-time or near-real-time from any of the software, hardware, devices or appliances that produce such information. Proposed solution should not be built on any opensource components and all components should be proprietary to the OEM.	
76.2		Proposed solution have the ability to natively monitor layer 7 traffic and perform deep packet inspection (DPI). Solution should support full packet capture and should have the ability where download packets can be restricted based on user/group. Proposed solution should not use any SQL or Flat files or RDBMS database for storing logs and events.	
76.3		Solution should have the capability of doing Log Filtering as all logs are not needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.	
76.4		The Proposed solution must offer all of the below built-in threat detection techniques out of the box:	
76.5		Detect Web Application Threats & APT Threats	
76.6		Detect Threat indicated by advisories	
76.7		Give visibility of endpoints also by integrating with EDR, Antivirus etc for endpoint anal Integrate with leading NBAD tools.	
76.8		There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	
76.9		Machine learning should be embedded across the platform (SIEM, SBDL). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & perdict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate advanced ML frameworks.	
76.10	Correlation & Dashboarding	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		performed across all the different data sources including but not limited to logs. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle. The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.	
76.11		The proposed solution must support the data replication natively without relying on other third-party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artefacts for any incident analyst is working on. The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.	
76.12		The proposed solution must be able to capture all information in the original event data, logs and alerts including payload information and redisplay them for purposes such as troubleshooting, analysis and other data processing needs. The proposed solution must be able to support caching mode of transfer for data collection, so as to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection. For future proofing, proposed solution should be able to take feeds from proposed / existing SIEM & proposed / existing EMS solution.	
76.13		Next Gen Big Data Analytics platform should be sized to ingest data of 1Tb/ day in the form of logs, events, metrics and traces. Security monitoring solution should be sized for sustained data of 500 Gb/day at all layers but should be able to handle peak of 1 Tb/ day at all layers without dropping events or queuing events. There should	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users or data source count changes, till the time data ingestion size remains 500 GB/ day.	
76.14		The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize its response to help ensure effective incident handling. The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem.	
76.15		Solution should able to maintained native logs so that they can be used as evidence/ records, for legal proceedings and forensic analysis. Solution should be able to address forensic analysis with ability to correlate any machine data. The solution shall provide full forensic event playback to ensure comprehensive trend and historical analysis and reporting. The solution shall support backup and restoring security logs in a different location for incident handling and/or forensic investigation purposes. Solution must be able to build an unstructured index or store data in it's original format without any rigid schema.	
76.16	Monitoring & Management	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required. The proposed solution must provide a query interface that allows users to search for data stored within the solution.	
76.17		Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration. Proposed solution should be provide a single console view where we can see all data whether metric or log event data and have a capability to correlate between the data sets.	
76.18		The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing url parameters to any third party website. The Report should be scalable IP-wise, device-	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		wise, user-wise, data-wise, location-wise based on requirement between any two dates.	
76.19		Proposed solution must be able to create alerts to notify about suspect activities, allowing actions like: enriching data, sending email, sending information to a syslog and exporting a PCAP file that may be accessed via CIFS/SMB/NFS and via dashboard. Solution should provide the ability to choose between capturing all packets and selective packet capture to lower storage requirements	
76.20		Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And Out of box aging analysis of incident should be available.	
76.21		The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The Dashboard should be accessible from the endpoints as & when required.	
76.22		The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click.	
76.23		The solution must dynamically learn behavioral norms and identify and report on changes as they occur by baselining the the customer environment and monitoring for changes from a known normal state.	
76.24		Proposed solution should come with out-of-the-box dashboards through which you can see the status of key KPIs over time. Solution should allow you to identify the trends or specific points in time where KPI status changed and drill down to the health page where we can monitor metrics like CPU usage, average memory usage, average datastore latency and average network traffic across all hosts.	
76.25		Proposed solution should be able to analyze the health of your infrastructure. It should have the capability to look across different infrastructure types and identifies the inactive entities that could	

VERIFIED

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		be causing issues in the production environment.	
76.26		Solution must be able to analyze captured traffic and PCAP files simultaneously. The proposed solution must support the decoding of the following network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/ AD, PostgreSQL, Sybase/ SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI	
76.27	Incident Management	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle. The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel.	
76.28		The proposed solution must provide investigation auditing capability to enable analysts to easily: a) Track searches and activities b) Review activities at any point c) Select and place into timeline for temporal analysis d) Help remember searches, steps taken, provide annotation support	
76.29		The centralized view must be able to streamline investigations and accelerates incident responses by centralizing artifacts and context from endpoint, network and all other logs, events and security data relevant to an incident.	
76.30		The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availablity status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard	
76.31		The proposed solution should have OOTB support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		are required to implement MITRE ATTACK Technique & Sub techniques.	
76.32		The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should also be capable of being used for SBDL & SIEM. Solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface. Old data should be parsed with new parser without re ingesting or re-indexing the data.	
76.33	Machine Learning & Security Analytics	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the guided experience and should be able to integrate with generic machine learning tools.	
76.34		The proposed solution should have machine learning platform embedded in the solution that can easily help to build, built-in or create unlimited custom machine learning models using the pre-defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools.	
76.35		The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries.	
76.36		The proposed solution machine learning capabilities must includes API access, role-based access controls for machine learning models. The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.	
76.37		The proposed solution must provide the following capabilities as a Security Analytics Platform: One single syntax that can be used universally for search queries, alerts, reports or dashboards Incident review framework to facilitate incident tracking, investigation, pivoting and closure Risk scoring framework to apply risk scores to any asset or user based on relative importance or value to the business. Threat intelligence framework that automatically collect, aggregate, deduplicate	

VERIFIED

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		indicators of compromise from threat feeds	
76.38		The platform must provide a wide range of analytics models with capabilities such as: Analytics to detect conditions such as anomalous device behaviour patterns within peer groups, across time periods and rare behaviour patterns, Lateral Movement Detection, Exfiltration Detection, Reconnaissance Detection, Zero Day Detection, Ransomware Detection DNS based detection analytics for timely detection of botnet malware threat, Unauthorized Access Detection Analytics for scoring threats identified by third party solutions such as HIDS/HIPS, AV etc	
76.39		The proposed solution must be able to retrieve from any threat feeds without restriction, retrieve threats in various ASCII/UTF-8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and OpenIOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated eXchange of Indicator Information (TAXII). The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs and interfaced incl. text, XML, JSON and other evolving format.	
76.40	Integration	Should provide support to import logs from various Applications, perimeter devices and endpoints to SIEM solution and also create rules to correlate such logs. The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface. OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	
76.41	SOAR	The proposed solution must have a orchestrator ability to direct and oversee all activities from beginning to end with 2 user license with unlimited	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		actions. Proposed solution orchestrator must be able to ingest security data from any source and in any format. The proposed SOAR solution should have built in functionality for triage health check failures – perform ping test, gather information (VM status, OS uptime, SCOM status for Windows), and triage issues. The proposed SOAR solution should support periodic automations – notify the users of underutilized VMs and reduce VM profile. The proposed SOAR solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.	
76.42	Monitor, Alert & Reporting	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built. The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs. The proposed solution must possess built-in function for Predictive Analysis: Uses historical data as a baseline to forecast future patterns, thresholds and tolerances Ability to identify the future needs of critical system resources, no prior knowledge in predictive modelling algorithms required to use this functionality, and the ability to easily interpret and customize the results The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers. It should quickly compare resources and capacity utilization across many hosts The proposed solution must possess built-in feature for anomaly detection:	

Sl.	Category	SIEM & SOAR Technical Requirements	Compliance Yes/ No
		Uses historical data as a baseline to forecast future patterns, thresholds and tolerances Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results The proposed solution report or table must be able to be embedded in third-party business applications. The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. The proposed solution must be fully integrated with the log platform without the need to duplicate the collected raw logs The proposed solution must be able to read data input from the following log file formats: a) Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b) Windows Events Logs c) Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc. The proposed solution must be able to accept the following live data streams feeding through the network: a) Syslog Messages b) Security Alerts c) JSON streaming over HTTP/HTTPS	

77. **<u>C26 – NGFW Appliance</u>**

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
77.1	Perimeter Firewall	Hardware Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit	

<u>*VERIFIED*</u>

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
			operating system to support higher memory.	
77.2			Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.	
77.3			Firewall should have integrated redundant hot-swappable power supply	
77.4			Firewall should have integrated redundant fan tray / modules	
77.5			High Availability Configurations shall support Active/ Passive and Active/Active	
77.6		Feature Requirement	Should support performance as per the annexure for NGFW (FW, AVC, anti-bot, identity awareness, anti-malware, anti-spam, zero phishing and IPS) real-world/ production/ Enterprise Testing performance	
77.7			Firewall should support static NAT, dynamic NAT, dynamic pat	
77.8			Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
77.9			Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6/ IPv6 BGP	
77.10			Should support Multicast protocols like IGMP, PIM, etc	
77.11			Should support more than 8000 (excluding custom application signatures) distinct application signature as application	

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
			detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency	
77.12			Should support more than 12,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
77.13			Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
77.14			Should support minimum 5 Virtual Systems from day 1 and scalable upto 50 virtual system without any additional hardware.	
77.15			Should be capable of detecting and blocking IPv6 attacks.	
77.16			The solution should be able to identify, decrypt and evaluate both inbound and outbound SSL traffic on-box. Throughput of device with SSL inspection need to be mentioned by the Vendor and document /datasheet reference to be given.	
77.17			Should support threat intelligence feeds integration in standard formats (like STIX)	
77.18			The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network	

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
			probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
77.19			Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
77.20			The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques/ IoC based detection.	
77.21			Should be capable to give Minimal false positives with the behavioural/ ML based analysis technology or equivalent Real-time signatures and selective challenge-response mechanism for high mitigation accuracy should be possible	
77.22			Should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Real time Attack footprint should be visible to the administrator for forensics purpose.	
77.23			Network-flood/ threat protection should include:	
77.24			TCP floods which include SYN Flood,	
77.25			UDP flood/ signature for DNS based data exfiltration.	
77.26			ICMP flood/ ICMP based attacks	

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
77.27		Management Solution	The hardware based management platform must provide a highly customizable dashboard. Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant policy segment for an autonomous system	
77.28			The hardware management platform must provide centralized logging and reporting functionality. Logs should also be provided in standard formats which can be integrated with SIEM	
77.29			The hardware management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
77.30			Should support troubleshooting techniques like Packet tracer and capture.	
77.31			Should support REST API for monitoring and config programmability	
77.32			The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
77.33			The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
77.34			Solution should be able to provide insights of hosts/user	

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
			on basis of indication of compromise, any license required for this to be included from day one.	
77.35			The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
77.36			The management platform support running on-demand and scheduled reports	
77.37			The management platform must risk reports like advanced malware, attacks and network	
77.38			The hardware management platform should be in HA and must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
77.39	Intranet Perimeter Firewall	Throughput (NGFW (FW,AVC and IPS) Throughput threat prevention with Anti malware, Antibot , zero phishing ,	25Gbps 15Gbps	

VERIFIED

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
		Anti-Spam		
77.40		Interfaces	8 X 10G SFP+	
77.41		Concurrent Sessions	30 Million or more	
77.42		Connections /Second	Minimum 400K	
77.43		IPS	Yes	
77.44		IPSec Tunnels	Min. of 1,000	
77.45		Storage, Memory, RU	Min. of 128 GB of RAM, SSD of 2x480GB Storage in RAID1. Should not consume more than 3 RU.	
77.46		Malware Defence Including protection from zero phishing by injecting java script in user browser File scrubbing	Yes	
77.47	Internet Perimeter Firewall	Throughput (NGFW(FW, AVC and IPS)	5 Gbps	
77.48		Interfaces	4 GE RJ-45 + 4 X10G SFP+	
77.49		Concurrent Sessions	8 Million or more	
77.50		Connections /Second	100K or more	
77.51		IPS	Yes	
77.52		IPSec Tunnels	Min. of 1,000	

VERIFIED

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
77.53		URL Filtering	Yes	
77.54		Malware Defence	Yes	
77.55		Storage, Memory, RU	Min. of 32 GB of RAM, SSD 200GB of Storage in RAID1. Should not consume more than 1 RU	
77.56	Industry Certification		EAL4+ / NDPP	
77.57	Anti-APT Hardware	Feature Requirement	The hardware solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created: Real-Time Prevention-unknown malware patient-0 in web browsing without any external integration or client Real-Time Prevention-unknown malware patient-0 in email without any external integration or client	
77.58			The hardware solution must be custom built Anti-APT Appliance should be inline solution (not out-of-line) and integrate with network perimeter security component devices like firewall/UTM and IDS/IPS.	
77.59			Protocols - The solution must be able to emulate executable, archive files ,documents, specifically within various protocols: HTTP, HTTPS, FTP, SMTP, CIFS, SMB v3 Multichannel & SMTP TLS	
77.60			The solution must provide both onsite and cloud based implementations	
77.61			The solution must support 3rd	

Sl.	Component Name	Categories	Perimeter NGFW Firewall Technical Requirements	Compliance Yes/ No
			party integration (public API)	
77.62			The solution must support deployment in inline mode	
77.63			The solution must support ICAP integration	
77.64			the solution would enable emulation of file sizes larger than 100 MB in all types it supports	
77.65			Offered solution must support zero trust threat prevention security policy to address the unknown day 0 attacks by remove exploitable content, including active content and embedded objects for both email and web traffic integrated from day one. The solution should be able to reconstruct files with known safe elements.	
77.66			The solution must provide the ability to be centrally managed.	
77.67			Upon malicious files detection, a detailed report must be generated for each one of the malicious files.	
77.68		Hardware Requirement	Unique files per hour: 4000 Form Factor: 1U Minimum CPU cores: 2 x 8 physical, 24 virtual Virtual Machines: 24 Storage: 1x2000 GB SSD Memory: 128 GB Ports: 2x 10/100/1000 RJ45 and 2x with Included 10GbE SR transceivers for future expansion.	

78. **C-27 - Network Detection & Response**.

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
A	**Functional Requirements**	
78.1	The solution should be on premise and should not require internet access for day to day functionality. Any required update should be supported offline.	
78.2	The solution should support continuous full packet capture, for intended traffic (not just malicious traffic) to enable forensic investigations and threat hunting without the need for any 3rd party solution integrations	
78.3	The solution should natively support analysing raw network packet data, including UDP traffic, from layer 2 to layer 7 of the OSI stack for complete threat analysis. Solution Should not be limited to only Sampled or meta-data (e.g. IPFIX or NetFlow) analysis.	
78.4	The solution should provide an analysis of managed and unmanaged devices independently without requiring any integration with other solutions like Active Directory, identity solutions, NAC, EDR etc.	
78.5	The solution should provide an independent and comprehensive analysis of the attack surface by uniquely identifying and profiling endpoints (managed, unmanaged and IOT) based on behavioural fingerprints without depending on other endpoint solutions.	
78.6	The solution should support profiling and tracking endpoints (managed and unmanaged) irrespective of IP address changes, location change, lack of MAC address visibility or login credentials change, purely with just packet analysis and without the need for any external data source such as Active Directory, Configuration Management Databases (CMDB), endpoint solutions etc. The solution should not be dependent on MAC addresses visibility of devices for device profiling.	
78.7	The solution should have capabilities to identify historical information about all the endpoints (including unmanaged and IOT, if any) including information about user logins. This must be done without the need to integrate with any other solutions such as Active Directory or endpoint solutions. The solution should support search for user or device names.	
78.8	The solution should have capabilities to automatically group similar devices together for forensic and outlier analysis without requiring access to Active Directory or CMDB systems. The solution should have capability to group devices based on a combination of fingerprints, provide an explanation of the similarity and identify packet captures corresponding to those fingerprints.	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.9	The solution should have the capability to distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) drawn exclusively from network packets and without requiring integrations with other systems such as Active Directory, endpoint security and / or CMDB. The solution should have capability to track back to the actual traffic matching the fingerprint.	
78.10	The solution should be able to identify malicious activity by tracking commonality & frequency without requiring a baseline or training period.	
78.11	The solution should not depend exclusively on static rules such as IDS signatures, Suricata or Yara rules for threat detection. The solution should use artificial intelligence- based approaches to detect attacks.	
78.12	The solution should support and provide examples at a minimum all of the following data science methods: ● Supervised machine learning ● Unsupervised machine learning ● Deep neural networks ● Belief propagation ● Multi-dimensional clustering ● Decision tree classification ● Outlier detection	
78.13	The solution should natively provide details on domains accessed from the environment including date of first and last access, WHOIS information, subdomains accessed, protocols used, and bytes transferred, per device. The domain should have a risk score and domain category listed.	
78.14	The solution should maintain an updated 90-day profile of all devices including a summary of protocol history to aid in the discovery of low-and-slow attacks.	
78.15	The solution should detect threats in encrypted traffic without the need to decrypt. For example, the solution should check the commonality and frequency of TLS ciphers and destinations, without requiring support from existing network switches, endpoint agents or network proxies.	
78.16	The solution should have search capabilities that allow the end user to search over a minimum of 90 days of traffic history for IP addresses, domain, username, email addresses or device names. All advanced analytics capabilities should be supported for all devices with the ability to query a minimum of 90 days of history.	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.17	All components of the solution including all the software components, hardware components (sensor appliances, analytics Engine appliance, Analyst dashboard appliance, etc) and service & support should be directly from the same OEM.	
78.18	The solution should have an advanced search feature that allows the end user to search for any metadata field value combination including: ● Mac Address ● TLS Cipher suite ● TLS Server Name ● TLS certificate fields ● Web browser version ● JA3 value	
78.19	The solution should be able to classify applications and protocols across multiple protocol families for e.g. ● Application Family-Description ● Database-Protocol used for database remote queries ● Encryption protocol ● Tunnelling protocol ● Web-Generic web traffic ● Webmail-Web email application	
78.20	The solution should natively detect data exfiltration via methods including but not limited to DNS or ICMP tunnelling.	
78.21	The solution should natively detect command and control to web domains that are rare in the customer environment without relying on indicators of compromise, web reputation systems or threat intelligence.	
78.22	The solution should natively detect malicious browser extensions (man-in-the-browser attacks) that can be used to steal sensitive and private data without the need for any endpoint agent or integration with any other solutions, to provide an independent threat assessment.	
78.23	The solution should natively detect the use of defence evasion techniques such as proxy usage to hide data exfiltration and user agent spoofing to hide the source application.	
78.24	The solution should natively detect when attack tools are shared over SMB (file share).	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.25	The solution should natively detect indicators of compromise and early warning signs of ransomware such as the use of doppelganger domains, inbound remote desktop, clear text passwords, unauthorized use of remote management tools, etc.	
78.26	The solution should natively detect living-off-the-land attacks that use tools such as PSExec, PowerShell, WMI, remote registry etc.	
78.27	The solution should natively detect use of remote management tools from non-admin devices without the need for manual tagging of devices.	
78.28	The solution should fully expose the definitions for all the vendor provided threat detection techniques (models) and allow for their easy modification or adaptation.	
78.29	The solution should support a fully transparent and extensible language for building custom threat detections based on a minimum of 1000 attributes including but not limited to network protocol information, device information, behavioural fingerprints and similarity analytics, domain information, threat intelligence etc.	
78.30	The solution should provide a minimum of 300 reusable building blocks that can be composed into models for custom threat hunting. These building blocks should function as components (e.g. for detecting specific attacker tactics etc.) that end users can leverage to build models without the need for data science experience. All detection models and building blocks (whether provided by the vendor or the community) should be supported by the vendor.	
78.31	The solution should support automated and manual threat hunting, triage & investigations by surfacing the appropriate information needed by the security team. The solution should also allow the security team to add additional context and information to automated threat reports.	
78.32	The solution should support analysis of network traffic without the need to decrypt and without the need for any endpoint agents or additional solutions.	
78.33	The solution should natively support extraction of a single PCAP based on a device, particular network activity, threat etc. irrespective if the device has changed IP addresses, time elapsed etc. This capability should be accessible through the user interface and the APIs.	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.34	The solution should detect the use of unencrypted credentials on the network, passwords stored in unencrypted formats as well as the use of insecure protocols.	
78.35	The solution should support tagging and annotation of 1 or more critical devices with a single operation. The solution should also support the use of these tags for the purpose of building custom threat detection or compliance models.	
78.36	The solution should detect Kerberos brute force attacks and capture the client name, server name, and error message for all Kerberos requests (not just attacks) and store these details for at least 90 days in a searchable format.	
78.37	The solution should detect DNS tunnelling attempts and allows the end user to easily change the detection parameters based on record type (MX, TXT, CNAME, A), DNS recursion, TTL and other criteria.	
78.38	The solution should monitor, track and extract field value from LLMNR traffic and DCERPC traffic.	
78.39	The solution should monitor, track and extract field:value from SMB traffic, e.g - Kerberos Principal - NTLM Server DNS Domain Name - NTLM Workstation - Directory Query filter	
78.40	The solution should identify ransomware, executables, and other file types that are transferred via SMB file shares. The solution should be able to create a custom file share detection model based on end user file names.	
78.41	The solution should detect DCERPC enumeration techniques, such as: services enumeration, computer name enumeration, domain groups enumeration, password policy enumeration, and remote file process execution.	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.42	"The solution should have a native incident management workflow component with built-in automation that automatically: ● Visually maps out the devices and external destinations involved in the incident ● Visually maps the relationships between the devices involved. ● Automatically generates an incident of the attack when new traffic is added. ● Provides a PDF report that can be independently shared outside the solution. These capabilities must be natively provided without requiring other solution/integration	
78.43	The solution should support customizable dashboards that can be:● Assigned to individual users● Emailed on a scheduled basis● Exported as a PDF to share outside the system	
78.44	The solution should support retrospective detection and hunting for threats for a lookback period of up to 90 days, even if the traffic was assumed to be benign in the past.	
78.45	The solution should support a RESTful API and syslog forwarding to push alerts to ticketing systems and other 3rd party systems in order to assist workflow management.	
78.46	The solution should support integrations with at least 2 other leading SIEM solutions from different OEMs.	
78.47	The solution should support integrations with at least 2 other leading EDR solutions from different OEMs.	
78.48	The solution should provide a RESTful API to allow endpoint detection & response (EDR) and security orchestration (SOAR) to implement response actions.	
78.49	The solution should provide a RESTful API to support packet capture (PCAP) export.	
78.50	All required licenses for 3rd party integration should be included in the solution from day 1. Any integration that may be required in future should not be of any additional cost, for the duration of the contract.	
78.51	A single solution instance should be able to support 10Gbps of raw network traffic throughput without any licencing restriction on number of endpoints supported	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.52	Separate solution instances to be provisioned for Internet and Intranet across DC, DR and NDR (i.e. 6 instances in total)	
78.53	The solution should store all packet captures at the Sensor and only forward minimal metadata to the analytics engine(s).	
78.54	The solution should have scalable architecture to add more sensors and analytics engine in future.	
78.55	The solution should provide full functionality based solely on the capture and analysis of raw traffic, without requiring other inputs such as Netflow/Sflow, logs, APIs, endpoint agents or other integrations, to get an independent security view of the infrastructure during outages or attacks.	
78.56	All licencing should be quoted along with the product to meet all the technical specifications. Any new software upgrades, features and threat detection models that come out in the future and should be available at no additional cost for the duration of the contract.	
78.57	The solution should include onsite OEM professional services	
78.58	The OEM professional services to perform solution design and deployment.	
78.59	The OEM professional services to build custom detection models for customer's specific use cases, provide playbooks for network investigation and analysis.	
78.60	The OEM professional services should share methodologies for network threat hunting, should provide knowledge transfer and handover training.	
78.61	The OEM professional service should provide network forensic analysis to support the customer incident response team.	
78.62	The proposed product OEM should have a registered office and TAC Centre in India.	
B	**NDR input TAP**	
78.63	1:N data mirror function should be supported with max latency of 6ns. Device Should regenerate the signal in the original cable path and in the mirrored path.	
78.64	The device should be capable of converting between different media types on source, destination and mirrored path.	
78.65	Device should have redundant hot swappable fans and redundant hot-swappable power supplies	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.66	should have inbuilt tools like wireshark/tcpdump for troubleshooting	
78.67	Device should support PRBS bit level testing to verify link quality and transceiver operation	
78.68	Device should support LLDP for neighbour discovery	
78.69	The device should have a minimum 96 numbers of 1/10G native ports. All ports activated and populated with 10G-SR from day-1.	
78.70	Device should have capability to aggregate traffic from multiple input ports to single output ports	
78.71	The device should support at least 4 aggregate streams (mirror sessions/object) each capable of taking inputs from different ports.	
78.72	Device should be capable of packet timestamping with minimum resolution of 20 picosecond and precision of less than 1ns.	
78.73	Device should support deduplication of packets when aggregating multiple streams	
78.74	Device should have minimum 32GB of deep packet buffer to prevent frame loss when aggregating traffic from multiple ports to single output stream	
78.75	The device should have capability of packet truncation to remove the payload and pass on only the header (defined bytes) of the packet, to reduce aggregated bandwidth towards the monitoring port	
78.76	The device should support stream aggregation with jumbo frames upto 9K bytes for application monitoring using payload data	
78.77	Devices should support adding sequence number and deduplication hash in trailer extensions of packet.	
78.78	The device should support used definable rate limiting on aggregated traffic based on packet-rate and bandwidth.	
78.79	Device should support priority flow control between egress port and receiving device for aggregated traffic	
78.80	Device should support interface beacon for ease identification of the ports physically	
78.81	Device should have minimum 8GB of RAM and 64GB SSD.	
78.82	The device should have at least 2 nos of management ports, for separation of PTP and Management network.	
C	**NDR Input tap Aggregator**	
78.83	The device should support multiple M:N Tap to tool mapping simultaneously.	
78.84	The device should be capable to support same port working as tap port (Rx) and tool port(Tx) simultaneously	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.85	The device should have capability of packet truncation to remove the payload and pass on only the header (defined bytes) of the packet.	
78.86	The device should support GUI based management centrally as well as on the device	
78.87	The device should have 48 nos of 1/10/25G SFP28 and 8 nos of 100G QSFP28 ports. All ports should be activated and populated with MM transceiver from day-1.	
78.88	The device should support mixed speed port-channel i.e. active-active forwarding on LAG links consisting of multiple speeds e.g. 1G and 10G.	
78.89	The device should have support for packet timestamping	
78.90	The device should have deep packet buffers of 4GB or more to absorb burst traffic minimizing packet drops for N:1 tap port to monitor port scenarios	
78.91	The device should support minimum 20K or more Access Control Entries for packet filtering	
78.92	The Device should support ACL based traffic filtering.	
78.93	The device should support policy based traffic steering towards output ports, using ACL rules.	
78.94	Device should support traffic steering based on matching inner headers fields for GRE encapsulated traffic	
78.95	The device should support traffic steering based on MPLS label value.	
78.96	The device should support header striping for 802.1q, MPLS, VXLAN, 802.1BR and VN-tag	
78.97	The device should support vlan tag or similar mechanism to specify input interface in outgoing packet towards tools.	
78.98	The device Should have Virtual output Queue based architecture to avoid head of line blocking issues	
78.99	The device should support PTP 1588 transparent mode and boundary mode	
D	**NDR Input tap & tap Aggregator Common Requirement**	
78.100	Each single solution instance of NDR must include 2x TAPs devices and 1x TAP Aggregator device.	
78.101	All tap & tap Aggregator device part of the solution should be able to provide automation and programming with native support for bash, and python	
78.102	All tap & tap Aggregator devices should support installation of user application with support for RPM install and docker containers	
78.103	All tap & tap Aggregator devices should support open config over RPC	

Sl.	Technical Requirements of Network Detection & Response	Compliance Yes/ No
78.104	All tap & tap Aggregator devices OS should be modular supporting fault containment and stateful repair. All devices should be able to run same OS binary.	
78.105	All tap & tap Aggregator devices should support bug fix/Patching without rebooting the OS.	
78.106	All tap & tap Aggregator devices should support TACACS+, Radius and Role based access control	
78.107	All tap & tap Aggregator devices should support redundant hot swappable Power Supplies and redundant hot-swappable fans	
78.108	All tap & tap Aggregator Devices should support real time streaming telemetry for statistics and other parameters for monitoring from a same dashboard for monitoring and management. Required VM licencing should be quoted alongwith.	
78.109	The tap & tap Aggregator devices should be provided with unified monitoring, provisioning and telemetry solution from the same OEM. It should support telemetry with real time and historical time-series database view, traffic flow analytics, PSIRT & Bug visibility, configuration compliance, centralised patching & upgradation, Zero touch provisioning, resource utilization monitoring, event notification, Change workflow management, notification through email & msg, 3rd party integration. Required appliance/hardware should be provided along with.	
78.110	All required licensing for mentioned technical specification should be quoted along all the devices	
78.111	All devices should be provided with direct OEM TAC and OEM hardware replacement support.	
78.112	Optics should be from the same OEM as the devices' OEM.	
78.113	The OEM will provide onsite knowledge transfer and handover training	
78.114	All OEM Professional services should be provided by personnel(s) on OEMs payroll only.	
78.115	TAC support must be directly from the OEM with 24x7 TAC availability over email and Phone. OEM should have a registered office and TAC Centre in India.	

79. **C28 – IDAM Technical Requirement**

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.1		SOLUTION SPECIFICATIONS: GENERAL	
79.2		The proposed solution should have a central identity manager	

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.3		The multi datacentre authentication/access capability should be such that that the session created at one data centre should be synced and respected at a remote data centre while traversing from a locally protected app to a centrally deployed centrally protected application.	
79.4		Proposed Solution should have a LDAP Directory with Directory Replication Capabilities to maintain a read only copy in remote data centres.	
79.5		Solution should provide Single Sign On (SSO) with role based access control to users of application.	
79.6		The solution implemented should offer customizable landing page which can be accessible over Army Data Network. User once authenticated, the landing page should display the list of all applications authorized to him. On choosing any application, the user should be directed to that application with the correct credentials without having to separately login/ sign in. The page should also allow users to manage own attributes e.g. change password, contact details etc.	
79.7		Solution should integrate all websites/ applications deployed over ADN (approx 500) – to incl static/ dynamic websites and applications (predominantly web based)	
79.8		The proposed solution should be able to seamlessly integrate with existing Application	
79.9		Solution should have the capability to integrate with Active Directory.	
79.10		The solution should run in High Availability (HA)	
79.11		Solution should support integration with the applications running across different web/ application sever which will be hosted on different OS such as Windows/ Linux/ Solaris.	
79.12		The sys software should be completely scalable to accommodate the changing Nos of users and applications.	
79.13		System shall have complete web based administration module	
79.14		The proposed solution should be FIDO Compliance	
79.15		Support for interoperability with cross platforms specifically Windows and Linux	
79.16		IDENTITY and ACCESS MANAGEMENT SOFTWARE provider should be certifying authority under CCA	
79.17		Support SSL/ TLS of latest version	

VERIFIED

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.18		Solution should have undergone third party Vulnerability Assessment and Penetration Testing (VAPT) and proof of audit certificate should be produced	
79.19		Support distributed, offline mode in containerised deployment for Ships, remote offices	
79.20		Support API integration to get dynamic, on-the-fly group member data from external APIs	
79.21		SPECIFICATIONS: IDENTITY MANAGEMENT SOFTWARE	
79.22		Management of Identity profiles should be central with a single repository of identity data.	
79.23		Entire management of identities should be web based.	
79.24		Solution should be able to create, update, and delete user accounts across the enterprise environment both manually and automatically.	
79.25		The solution should enable assignment of users to single/ multiple roles.	
79.26		The solution should have a workflow for provisioning/ de-provisioning of identities.	
79.27		Solution should provide a graphical interface that allows creating and managing workflows.	
79.28		Solution should automatically route access requests of users for approval to the destined administrator.	
79.29		Solution should have ability to delegate approval authority to another person.	
79.30		Solution should have ability to escalate a request to an alternative approver if the allotted time elapses.	
79.31		Provisioning solution should provide capability to the approver to provide comments.	
79.32		Should support withdrawal of non-approved requests	
79.33		Solution should be able to generate unique user IDs.	
79.34		Should integrate with PKI to complete user creation process.	
79.35		Solution should provide auto requisition of PKI token personalization for new users being created	
79.36		Should support provisioning/ de-provisioning on joining/ movement of personnel on transfers and temporary assignment of roles.	
79.37		Solution should provide delegated administration.	
79.38		Solution should be able to define delegated administration by way of both administration (which users, which resources) and capabilities (full account administration, password administration only, etc.).	

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.39		Solution must support web-based self-service in terms of changing passwords, resetting forgotten passwords retrieving forgotten user login etc	
79.40		Solution must allow users to view their profile and the resources and the corresponding entitlements they have got access to.	
79.41		Must have capability to provision user accounts to target systems and applications.	
79.42		Must have out-of-box connectors available for target systems to carry out user provisioning and reconciliation operations.	
79.43		The proposed solution should more then 15 Factors of Authentication based on policies defined	
79.44		Should have connector development framework to extend support to additional target systems for which out of box connectors are not available.	
79.45		Should have capability to allow administrators to define and enforce global password policy that includes password composition rules like -minimum length- minimum password age- warn after expires, disallow past passwords	
79.46		Should support complex password rules including maximum repeated characters, minimum numeric characters, alphanumeric characters, uppercase & lowercase characters etc	
79.47		Should support validation of password provided against the defined password policy.	
79.48		As part of forgotten password, the solution should have support to challenge the user for security answers to the questions that must have been configured at the time of user creation or self-registration. The manager of the user whose password is being reset must be notified of this password reset.	
79.49		Solution should allow users to manage their own passwords.	
79.50		Should have ability to synchronize passwords for multiple systems to the same value to reduce the number of different passwords to be remembered by the user.	
79.51		Should support delivery of password-change success/ failure status to requestor using mechanisms like email	
79.52		Users should be able to update personal attribute information, such as address, cell phone number, etc.	
79.53		Solution should provide a web based front-end for help-desk administrators to use.	

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.54		Solution should provide a password exclusion list and allow restriction of using old passwords.	
79.55		Solution should support Role Based Access Control (RBAC).	
79.56		Solution should report on who had access to what on a given date.	
79.57		Solution should support the creation of custom audit policies (eg. Separation of Duties) that can be applied during access scans.	
79.58		Solution should support reporting grouped by the following: By administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator) By platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on target platform) By workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time) By user (audit history per user, accounts/privileges by user, self-service activity by user)	
79.59		Should support reports related to access policy, request, certification, approval, role, organization, password, resource & entitlement, user.	
79.60		Should support reports like list of all the rogue accounts existing in a resource, list all orphaned accounts etc.	
79.61		Should support SSL/TCS digital certificate based secure encrypted communication.	
79.62		Solution should not impose a physical or logical limitation on creation of number of users, while concurrency factor will drive the proposed hardware.	
79.63		Solution should have the capability of configuring applications for single factor as well as multi factor authentication.	
79.64		The solution should support all types of web browsers like Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, etc.	
79.65		SPECIFICATIONS: ACCESS MANAGEMENT SOFTWARE	

Sl.	Category	IDAM Technical Requirements	Compliance Yes/ No
79.66		Should have capability to provide centralized logout	
79.67		Must support integration with PKI Technologies to support certificate-based authentication	
79.68		PKI and Digital Certificates is mandatory requirement for Ensure Legal Non-Repudiation	
79.69		Must support OSCP based live certification validation from the CA Authority under CCA	
79.70		Should support Certificate Validation against CRL Export Dump	
79.71		Must give administrators complete visibility and control over real-time user session data including ability to search for and terminate specific sessions	
79.72		Must support delegated administration at each data Centre location to have visibility on local users	
79.73		Should allow administrators to enforce constraints on session lifetime Idle timeout max number of concurrent sessions	
79.74		Should be compatible with a variety of web/app servers including Apache, IIS, IBM HTTP, Oracle HTTP, Node JS, Tomcat, JBoss, WebLogic, WebSphere	
79.75		Should have support to log authentication success and failure	
79.76		Behavioural and Risk based Parameter Detection for user-login to provoke authentication layers in line with real-time adjusted risk profile.	

80. **C29- Privileged Access Management (PAM)**.

Sl.	Category	Privileged Access Management	Compliance Yes/ No
80.1	Privileged Access Management	A Privileged Access Management should have:	
80.2		Fine Grained Access Control to protect their systems from unauthorized access and unintentional errors, if any. It allows restricting and controlling privileged users through a rule and role based centralized policy.	
80.3		Solution should have Password Vault which generates strong and dynamic passwords and the engine can automatically change passwords for several devices or systems at one go.	
80.4		SSH Keys: SSH keys reinforce an enterprise's authentication control management. SSH keys are valuable credentials to access privileged	

Sl.	Category	Privileged Access Management	Compliance Yes/ No
		account	
80.5		Solution should have Multi-factor Authentication. One-Time-Password (OTP) validation to begin a privileged session and the tool seamlessly integrates with disparate third-party authentication OATH and PKI based Authentication solutions	
80.6		Session monitoring enables IT security team to spot any suspicious activity around privileged account. Live Dashboard ensures that all critical activities performed by administrators across the IT infrastructure are viewed in real-time	
80.7		Auto-discovery should be able the risks management team to discover shared accounts, software and service accounts across the IT infrastructure	
80.8		Password Reconciliation should be capable for day-to-day administrative tasks become easy. Once the latest credentials from PAM, i.e IP Address, Port, Username and Password for a particular service is received, it should connects to the target device automatically using those credentials	
80.9		Virtual Grouping should provide a dynamic group setting with one to many relationships and virtual grouping.	
80.10		Solution should have Workflow for provision for administrator' configure the approval process for privileged users, user-groups and service groups. Service and password request workflow mechanism speeds-up the process of assigning target servers to privileged users	
80.11		Solution should have option to management for controlling and monitoring non-admin user activities that require temporary privileged access to the systems	
80.12		Solution should have Active Bridging between Linux machine and Windows AD Server	
80.13		Solution should enables administrators to auto provision and de-provision users or devices by interacting with active directory	

Sl.	Category	Privileged Access Management	Compliance Yes/ No
80.14		Solution provides centralized control point through which all network connections and traffic is routed for management and monitoring	
80.15		Solution should provide option for multi-tab feature which allows users and/or administrators to open multiple sessions in different tabs in the same window and allow them to switch between sessions as required	

81. **C30- Endpoint Protection, End Point Detection & APT**.

Sl.	Cloud Workload Protection	Compliance Yes/ No
81.1	Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server.	
81.2	Solution should support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control, and Recommended scan in single module with agentless and agent capabilities	
81.3	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should support CVE cross referencing when applicable for vulnerabilities.	
81.4	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	
81.5	Solution should have feature to take backup of infected files and restoring the same.	
81.6	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be part of the agent .	
81.7	Product should support CVE cross referencing when applicable for vulnerabilities.	
81.8	Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.	
81.9	Should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies)provide automatic recommendation of removing assigned policies if vulnerability no	

Sl.	Cloud Workload Protection	Compliance Yes/ No
	longer exists	
81.10	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems.	
81.11	Should have pre and post execution machine Learning and should have Ransom ware Protection in Behavior Monitoring.	
81.12	Demonstrate compliance with a number of regulatory requirements including PCI DSS, HIPAA etc.	
81.13	Should be Common Criteria EAL 2+ and FIPS 140-2 validated	
81.14	Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious	
81.15	Proposed solution should be Leader in Server Security Market as per IDC latest report	
81.16	Management of proposed solution should support both window as well as Linux platform	
81.17	Container security automated processes for critical security controls to protect containers and the Docker host. Bake security into the CI/CD pipeline for frictionless automation	
81.18	API-first, developer-friendly tools to help you ensure that security is baked into DevOps processes	
81.19	Should automatically submit unknown files/suspicious object samples with On-Premise sandbox solution for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to server security	
81.20	Solution should bring advanced protection to physical and virtual servers. It should support automatic policy management, and in the case of virtualised environment like VMware NSX-V® and VMware NSX-T™ -integrated agentless security, solution shall enable easy deployment and management of security across multiple environments.	
81.21	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and Solution Should have pre and post execution machine Learning and should have Ransom ware Protection in Behavior Monitoring.	
81.22	The proposed solution should be deployed in minimum 5 Govt/PSU/Defence customers for the last 5 years with similar deployment size as asked in the tender. Supporting document like Purchase order copy/Invoice should be submitted alongwith the bid response.	
Anti -Advance Persistent Threat		

Sl.	Cloud Workload Protection	Compliance Yes/ No
81.23	Proposed hardware should be a purpose-built hardware specific to the requirement.	
81.24	It should have redundant power supply.	
81.25	Hardware should have management port for the configuration and troubleshooting activities, management port should have 10/100/1000 base-T RJ45 port x 1 iDrac enterprise RJ45 x 1 interface available.	
81.26	Solution must be a custom built on premise Anti-APT solution and must not a network perimeter security component part devices like UTM/NGFW to improve the performance.	
81.27	The proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, RLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard.	
81.28	The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable.	
81.29	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment having detection capability of lateral movement (attack activities) inside the network (beyond C&C connections). Solution should have capability to detect zero-day threats, embedded exploit code, rules for vulnerabilities and enhanced parsers for handling file deformities.	
81.30	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with more than 90 protocols for inspection.	
81.31	The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session having 1 Gbps throughput inspection capability.	
81.32	The proposed solution should be able to store packet captures (PCAP) of malicious communications detected by sandbox and should be deployed on premise along with on premise sandboxing capability.	
81.33	Proposed Solution shall have extensive detection techniques with capability to analyse web, IP, mobile application reputation in addition to heuristic analysis, perform advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits.	
81.34	Solution shall have capability to perform advanced threat scanning and does correlation with multiple protocols to detect advanced malware and to capture malware behvaiour	

Sl.	Cloud Workload Protection	Compliance Yes/ No
81.35	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: pdf, exe files, compressed files , .jpg, .dll, .sys, .com and .hwp, .bat, .cmd, .cell, .chm, .csv, .class, .cla, .dll, .ocx, .drv, .doc, .dot, .docx, .dotx, .docm, .dotm, .cpl, .exe, .sys, .crt, .scr, .gul, .hta, .htm, .html, .hwpx, .iqy, .jar, .js .jse, .jtd, .ink, .mov, .pdf, .ppt, .pps, .pptx, .ppsx, .psl, .pub, .rtf, .slk, .svg, .swf, .vbe, .vbs, .wsf, .xls, .xla, .xlt, .xlm, .xlsx, .xlsb, .xltx, .xlsm, .xlam, .xltm, .xml, .xht, .xhtml, .url and extensive File Types i.e. Compressed Files (7z, rar, zip, cab, jar, gz, tar, bz2), Script Based (bat, ps1, vbs, js), Executables (exe, dll, scr) and Office Documents / PDF (doc /docx, ppt/pptx, xls/xlsx, pdf, mdb).	
81.36	Proposed solution should be able to provide customizable sandbox to match customer's environments.	
81.37	The Proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm etc. simultaneously on a single appliance having capabilities to configure files, IP, URLs and Domains to Black list or white list.	
81.38	The proposed solution should be able to run at least 20 parallel sandboxes images scalable up to 60 for analysis of payload having 2 TB in RAID 1 of on box storage from day one with a scalability of 8 TB.	
81.39	Proposed solution should support STIX/TAXII, Data Exchange Layer (DXL) and Restful API for sharing threat intelligence with other vendor products.	
81.40	Customized sandbox solution should support following operating systems (Win8/8.1, Win 10, Windows Server 2008, 2012, 2016 and Linux).	
81.41	Should perform static and dynamic analysis to identify an object's notable characteristics: Autostart configuration, self-preservation, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, process, service, or memory object change and Rootkit, cloaking, suspicious network activity.	
81.42	Should detect form targeted attacks and advanced threats targeted and ransomware attacks, Zero-day malware and document exploits, Attacker behaviour and network activity, Web threats, including exploits and drive-by downloads, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive applications highlight reports including infections, C&C behaviour, Lateral Moment, Assets and data discovery and data exfiltration.	

Sl.	Cloud Workload Protection	Compliance Yes/ No
81.43	Access different information about affected hosts on the following views: Displays a summary of affected hosts by attack phase, provides access to host details views and displays host event details in chronological order.	
81.44	The Proposed APT solution should be International Computer Security Association (ICSA) certified and have achieved >99% effectiveness as per latest Advanced Threat Defense (ATD) Test Report.	
81.45	The Proposed solution should integrate seamlessly, also share Indicators of compromise for mitigation with different layers like server, endpoint for having common threat sharing platform to block zero day threat holistically.	
81.46	The Proposed Solution shall share the Intelligence of malwares/samples that are detected through sandboxing with existing server security solution in ICG to block the threat on servers automatically. There should not be manual intervention to run this integration.	
81.47	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviours for advanced threat detection.	
81.48	The proposed solution must be able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable.	
81.49	The Proposed solution should have option to share Indicators of compromise for mitigation with EPP at endpoint. Similarly Endpoint/Server Security should submit samples to anti-APT solution for analysis, and shall block the samples on a real time basis based on the Sandbox analysis.	

82. **<u>C31- Authorization, Authentication and Accounting (AAA)</u>**.

Sl.	Category	Authorization, Authentication and Accounting (AAA) Technical Specifications	Compliance Yes/ No
82.1	General	The Solution should provide a highly powerful and granular access control solution that combines authentication, authorization, and accounting (AAA) and TACACS of administrative users for the devices like switches, routers etc	
82.2		The Solution should enable logging and integration of AAA logs with SIEM or centralised logging solution to facilitate discovery of particular user account activity or enable search across logs for specific user details based on account name, time stamp etc.	

VERIFIED

Sl.	Category	Authorization, Authentication and Accounting (AAA) Technical Specifications	Compliance Yes/ No
82.3	TACACS	Solution should be scalable enough to support 200 Network Devices	
82.4	Features	It should be possible to group the access control of the users based on the role	
82.5		Solution should be able to control the commands that user is allowed or not allowed to run on CLI session. It should understand the wildcard and regex matching	
82.6	Accounting	Solution should support the logging of commands run on the CLI of various network/security devices	
82.7	NAC Features	Support for enterprise level policy based network and access management on devices and users	
82.8		Comply to 802.1x NAC standard	
82.9		Shall enforce device and user compliance	
82.10		Quarantine noncompliant device	
82.11		Shall enforce restricted access to devices depends on central policy	
82.12	Policy lifecycle management	Enforces policies for all operating scenarios without requiring separate products or additional modules	
82.13	Profiling and visibility	Recognizes and profiles users and their devices before malicious code can cause damage	
82.14		NAC Solution should strictly support pre-connect model and should not allow Endpoint into network to complete profiling or discovery of Endpoint.	
82.15	Guest networking access	Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal	
82.16		The solution should support flexible guest account approval even in absence of sponsor	
82.17	Security posture check	Evaluates security-policy compliance by user type, device type, and operating system. Should check for compliance including lack antivirus, patches, or host intrusion prevention software from accessing the network	
82.18	Incidence response	Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention	

Sl.	Category	Authorization, Authentication and Accounting (AAA) Technical Specifications	Compliance Yes/ No
82.19	Bidirectional integration	Integrate with other security and network solutions through the open/RESTful API	
82.20	Deployment Models	The solution should support centralized and distributed deployment options with clustering of nodes or cross-site failover for disaster recovery scenarios	
82.21		The solution should provide full TACACS+ capability including enable password, configuration present for different NAD types, TACACS+ proxy etc.	
82.22	Vendor agnostic	Shall support 3rd party L2 switches/ Network components compliant to 802.1x standard. The NAC solution should be standard RADIUS server with built-in certificate authority	
82.23	Integration Capability	The NAC solution should be able to integrate with Firewall, APT, NBAD and SIEM solution	
82.24	Offline support	Should support MPLS network outages for prolonged period (user configurable in hours) and Users/ Devices continue to access local network with NAC in the event of MPLS network outage with DC, DR DC	
82.25	NAC License	Solution should be provided with 2000 users licenses	

83. C32- PKI Solution

83.1. C32.1 PKI Certificate Manager

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.1	PKI Certificate Manager with Remote Signing	Platform support	
83.1.2		Solution Software must support Windows Server 2012 or higher or Red Hat Linux Enterprise 6 or higher.	
83.1.3		Solution Software must support MS SQL 2012 or Oracle 11g or any underlying RDBMS.	
83.1.4		Solution must support LDAP v3 directories, if user data is stored in an X.500 directory.	
83.1.5		A High Availability configuration should be supported with	
83.1.6		Redundancy throughout the server systems.	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.7		There should be a mechanism for monitoring, such as SNMPv3/ Syslog.	
83.1.8		Each component should create error logs with configurable log level and a well-defined syntax.	
83.1.9		CA features	
83.1.10		It should be possible to run any number of CAs in any hierarchy in the same system. The CAs should possibly have different CA policy	
83.1.11		It should be possible to assign registration officers to individual CAs or user domains and visibility/ usability of user data should be limited to assigned CA or user domain	
83.1.12		The CA should be able to publish CRLs and certificates in any number of distribution points using LDAP/HTTPS protocol. The publication address must be configurable for each CA	
83.1.13		CRLs should be supported with configurable format, issuing period etc. Mechanism should be in place for publishing revoked certificates on real time basis/ occurrence.	
83.1.14		OCSP should be supported with "immediate" revocation information, i.e. revocation information should be available without latency.	
83.1.15		End entity certification according to individual policies.	
83.1.16		Signature algorithms: RSA, RSASSA-PSS and ECDSA should be supported with SHA-2 of 256, 384 and 512. Key	
83.1.17		Algorithms should be supported with key lengths as SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 Key Algorithms: DSA, ECDSA, RSA and RSASSA-PSS.	
83.1.18		End entity key management: It should be possible to encrypt, archive and recover end entity private keys (typically encryption keys).	
83.1.19		Support of multiple HSMs (over PKCS#11 and JCE) for	
83.1.20		Storing CA private keys and all other system keys.	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.21		CA management	
83.1.22		The product must offer centralized, secure management of CAs, policies and configuration data with GUI support.	
83.1.23		CA key management, Root-CA and Sub-CA certification, CA policy management: It should be possible to manage any number of CAs in any hierarchy in the same system. The	
83.1.24		CAs should possibly have different CA policies	
83.1.25		It should be possible to define the CA policies with high granularity: certificate and CRL formats and contents, validity, revocation services (OCSP an d/or CRL and/or delta CRL, distribution point address), algorithms.	
83.1.26		It should be possible to define an individual policy for each CA	
83.1.27		Cross certification should be supported in both directions: internal CA to certify external CA and vice versa in PKCS#10 procedures.	
83.1.28		Policies for end entity certification (validity, certificate formats and contents, algorithms etc.) should be defined with high granularity for maximal flexibility. It should be possible to add private extension	
83.1.29		Certificate management interfaces	
83.1.30		SCEP should be supported. Only authorized (registered) SCEP devices should be granted with a certificate. Renewal over SCEP should be possible without an additional registration. It should be possible to run different SCEP services for different CAs.	
83.1.31		CMP should be supported – System should support certificate enrolment part of Certificate Management Protocol (CMP)v2	
83.1.32		There should be a powerful API (preferably Web Services protocol) that supports certification, revocation for any end entity as well as to retrieve user and certificate information. The API should be access controlled.	
83.1.33		Certificate and Credential Management	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.34		The system must support storing keys and certificates on smart cards, smart USB token, in PKCS#12 files and import them into the Windows certificate store of the end user device.	
83.1.35		The system issuance must support smartcard/ token	
83.1.36		The system must support delegated certificate issuing, revocation renewal	
83.1.37		Smart card and token products of leading OEMs/ Vendor must be supported and lock-in must be prevented by multi-Card and token Support	
83.1.38		forms should be configurable, e.g. number and purpose of certificates, key length, validity etc.	
83.1.39		The system must support end-user self-service functions for credential management tasks that can be performed by end users: PIN change, PIN unblocking, issuing, revocation, renewal, replacement as reasonable for different credential	
83.1.40		During certification and smart card/ token issuing, it must be possible search and retrieve user data from one or more LDAP type of directories.	
83.1.41		Delegated credential management and end-user self- services should be supported over a web based GUI. Delegated credential management should be possible without PKI support	
83.1.42		It should be possible to notify users (managers and end users) about tasks they should do due to various events, like if their certificates are about to expire, they receive new credentials, etc. If applicable, notifications should include an URL to visit the appropriate service resource. Notifications	
83.1.43		There should be alternative authentication methods to log in to the delegated management system in case of emergency (card not available, expired, PIN forgotten etc.) The services that can be used must be configurable according to the assurance	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
		level of authentication	
83.1.44		The input fields displayed in the Registration Authority client should be configurable so that selecting a different Token/ card procedure can change the fields displayed and/or the look of the input fields panel.	
83.1.45		**Security**	
83.1.46		With GUI support, it should be possible to define roles with various permissions (CA management, end entity management, audit, registration, publication, revocation, key recovery, etc.) and assign users to role.	
83.1.47		Access to data and services should be controlled according to roles	
83.1.48		Users are required to authenticate with certificate-based strong two-factor authentication	
83.1.49		All relevant user actions (e.g. registration, certification, revocation etc.) should be logged in a digitally signed revision safe audit trail (transaction log), which is audit-able. Relevant actions require commitment signatures of the user(s). Critical actions (e.g. CA management) require commitment signature of more than one officer	
83.1.50		The CA security architecture must underlie a successful security evaluation (like Common Criteria) and the Digital Certificate Lifecycle Management Solution should have undergone third party penetration testing/ ethical hacking tests and proof of audit certificate should be produced.	
83.1.51		System credentials should be confidentiality and integrity protected	
83.1.52		System configuration should be integrity protected.	
83.1.53		All sensitive tasks should require 4-eyes-principle	
83.1.54		Scalability and Reliability	
83.1.55		Should be scalable to at least 500 of hosted CA with support to multiple concurrent HSMs	
83.1.56		Should support Production rate of at least 250 certificate requests per second.	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.57		Should support Active-Active or Active-Passive type of high availability ensuring sub components that can be multiplied to match performance and fault tolerance needs.	
83.1.58		Should allow distributing Certificate Management services (certificate issuing, CRL generation, LDAP distribution, DB)	
83.1.59		to different physical/logical servers for greater scalability	
83.1.60		**Interoperability**	
83.1.61		Support for all relevant PKIX standards PKCS #1, #5, #7, #8,#9, #12, #15	
83.1.62		Support for different certificate profiles based on X.509 Public Key Certificates.	
83.1.63		Support Cross certification and CA hierarchies with all major CA vendors and service providers.	
83.1.64		SDK to customize certificate enrolment, certificate revocation, card /token production to fit CRPF data network environment.	
83.1.65		**Interfaces**	
83.1.66		Web Services - Common interface (SOAP) to enable easy integration	
83.1.67		SDK - client API with Registration, authorization, all registration functions should be available	
83.1.68		SCEP - Simple Certificate Enrolment Protocol for network devices (Router, VPN, firewall, security gateway etc.)	
83.1.69		Certificate Management Protocol support for both Initial enrolment request and update requests for certificate renewal	
83.1.70		API: Plug-In interface for Registration Authority client	
85.1.71		**OCSP Specification**	
83.1.72		CA shall support an OCSP capability using the GET or the POST method for DSC issued	
83.1.73		CA SHALL operate OCSP capability to provide a response time of ten seconds or less under normal operating conditions	
83.1.74		OCSP responses MUST be signed by an OCSP Responder whose Certificate is signed by the CA or its sub CA that issued the	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
		Certificate whose revocation status is being Checked	
83.1.75		OCSP responder certificate and subscriber certificates shall comply with latest version of interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act	
83.1.76		**Time stamping server**	
83.1.77		ICG is required to operate Time Stamping Services as per CCA guideline	
83.1.78		The CA shall not issue a Time stamping certificate other than for its own time stamping service.	
83.1.79		Time stamp tokens shall be in compliance with RFC 3161.	
83.1.80		The time values the Time Stamping services used in the time-stamp token shall be traceable to a Standard Time Source in India	
83.1.81		Audit log files shall be generated for all events relating to the security of the Time Stamping services	
83.1.82		**Remote Signing (eSign)**	
83.1.83		eSign solution shall comply with existing and future Information Security Guidelines for Digital Signature Certificates and Adherence to Controller of Certifying Authorities Guidelines, Govt. of India.	
83.1.84		There should be powerful and secured API for easy interface with applications to enable eSign services	
83.1.85		The eSign API should take care of all the security aspects applicable Web Services and Web applications. The service should support encryption of all or part of Request and Response. The service should also ensure that the Hash data exchanged between the Indian coast gaurd and Service Provider should be encrypted and secure	
83.1.86		eSign Services should not be dependent on aadhar eKYC as per New CCA Guidelines. User can request for eSign by using offline KYC or any modes of KYC specified by CCA from time to time	

Sl.	Category	PKI Certificate Manager Technical Requirements	Compliance Yes/ No
83.1.87		Solution should allow placing the signature in the specified position in the document.	
83.1.88		Certificate and page configuration as per requirement	
83.1.89		Solution should support signing of multiple pages in the same document	
83.1.90		Should have facility of Co-Signing , means one document can be Digitally Signed by multiple authorities	

83.2. **C32.2- PKI Validation and ESigner**

Sl.	Category	PKI Validation and ESigner Technical Requirements	Compliance Yes/ No
83.2.1	Validation	Bidder should supply, install, test, commission, and maintain the Digital Certificate/ Signature based authentication solution for ICG application	
83.2.2		The solution shall comply with existing and future Information Security Guidelines for Digital Signature Certificates and Adherence to Controller of Certifying Authorities Guidelines, Govt. of India.	
83.2.3		The proposed solution should be provided with High availability (Active Passive) in primary and DR site.	
83.2.4		The bidder shall be responsible for complete end-to-end implementation of the solution, including the necessary changes, configurations, & customizations etc. in the existing ICG application	
83.2.5		The application should have a module for management of digital signature including issuance by CA, renewal and suspension of digital signatures based on the administrative decisions taken by the ICG.	
83.2.6		The Digital Signature solution shall be compatible with all browsers like Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, safari etc in all existing version. It should be compatible on all OS I e Windows, Ubuntu, Linux, Unix, MAC, Redhet and all	

Sl.	Category	PKI Validation and ESigner Technical Requirements	Compliance Yes/ No
83.2.7		The solution should have two components, the client side digital signing module (signer component) integrated with ICG application and server side digital signature verification module (verification component).	
83.2.8	Signing	The signer component deployed on the client side should be capable of restricting the use of Digital Signature from non-FIPS compliant USB Tokens thereby allowing use of only FIPS140-2(Level-2) compliant or higher grade USB tokens in the authentication process	
83.2.9		The signer component should latest available solution for digital signature in which no dependency on Java Applet, ActiveX or newer technologies like HTML5, WebSockets for wider adoption in multiple environments.	
83.2.10		The solution shall support real time digital signature verification and digital certificate validation including certificate expiry, trust chain validation and revocation checking.	
83.2.11		The signature verification component shall be able to validate certificate through Online and Offline CRL and OCSP.	
83.2.12	Signing	The solution shall accept X.509 v3 digital certificates issued by all licensed certifying authorities (CAs) in India.	
83.2.13		The system should allow officer to use digital signatures for signing the document in workflow wherever the digital signing is required.	
83.2.14		Multiple document can be signed at one time	
83.2.15		Should support signature of multiple person in single document.	
83.2.16		Audit log files shall be generated for all events relating to the Digital Signature. All security audit logs shall be retained and made available during Forensic requirement and compliance audits.	
83.2.17		Solution should be deployed into Enterprise Environment in to multi-tier architecture. It should support virtualized environment.	

83.3. **C32.3- -Hardware Security module Technical Requirements**

Sl.	Category	Hardware Security module Technical Requirements	Compliance Yes/ No
83.3.1	Hardware Security Module	Specification	
83.3.2		Should support Windows 2008 or higher, Linux	
83.3.3		Should comply to standards FIPS 140-2 Level 3 crypto boundary	
83.3.4		Key Exchange Symmetric Algorithm: AES, Triple DES (No separate license of Algorithm to be charged)	
83.3.5		Support for Hash Message Digest HMAC, SHA1 SHA2 (224-512)	
83.3.6		Support for various cryptographic algorithms: Asymmetric Key RSA (2048-4096 bits)ECDSA , ECC (No separate license of Algorithm to be charged)	
83.3.7		Random Number Generation –FIPS 140-2 approved	
83.3.8		Should Published API for various above functionalities for integrating with the Application software	
83.3.9		Keys must be stored and protected in Crypto memory of hardware within FIPS boundary of HSM	
83.3.10		On-board key generation, signing inside the HSM	
83.3.11		Minimum keys storage should be 10000 RSA keys of 2048 bits within FIPS 140-2 Level 3 certified crypto memory	
83.3.12		The backup and recovery of the all keys should be automatic (Without any backup device)	
83.3.13		The solution should also support automatic synchronisation of keys between deployed HSM Systems	
83.3.14		HSM should be capable of overall key management (creation, archival, destruction)	
83.3.15		HSM admin utility should have facility to create CSR file for DSC creation process	
83.3.16		Support for minimum 2000 Transaction per Second @ RSA 2048 bits	

Sl.	Category	Hardware Security module Technical Requirements	Compliance Yes/ No
83.3.17		Concurrent 100 private keys should be usable for Signing process	
83.3.18		HSM should be field upgradable upto 5000 TPS without changing the box	
83.3.19		HSM should have the capabilities of 4 partitions in single appliance	
83.3.20		Appliance shall be network (TCP / IP) based appliance	
83.3.21		Appliance should have 2 network ports 1 GBPS each	
83.3.22		Appliance should be 2U rack size	
83.3.23		Appliance should have dual redundant power supply	

83.4. **C32.4- PKI KMS**

Sl.	Category	PKI KMS Technical Requirements	Compliance Yes/ No
83.4.1	KMS	A key management system should be based on an agreed set of standards, procedures and secure methods for: procedures and secure methods for:	
83.4.2		Generating keys for different cryptographic systems and different applications;	
83.4.3		Issuing and obtaining public key certificates;	
83.4.4		Distributing keys to intended entities, including how keys should be activated when received;	
83.4.5		Storing keys, including how authorized users obtain access to keys	
83.4.6		Changing or updating keys including rules on when keys should be changed and how this will be done	
83.4.7		Dealing with compromised keys;	
83.4.8		Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived	
83.4.9		Recovering keys that are lost or corrupted	
83.4.10		Backing up or archiving keys;	
83.4.11		Destroying keys	
83.4.12		Logging and auditing of key management related activities.	

84. **C33 - IT Operations & maintenance Services**. As per details included in the succeeding parts of this Appendix.

85. **C34 - Non-IT Operations & maintenance Services.** As per details included in the succeeding parts of this Appendix.

86. **C35 - SOC Services**

Sl.	Category	SOC Services Technical Requirements	Compliance Yes/ No
86.1	Installation, Configuration & Support	Installation, configuration, integration with infosec software application including SIEM/ GRC, One-time payment, Qty. 01 No.	
86.2		Security incident management / analysis support, maintenance with onsite CISSP certified Security Analyst (01 No. on Working Hours), SOC Support Engineer (02 No. on 24x7 for DC SOC & 02 No. on 24x7 for DR SOC), Recurring quarterly payment on delivery of services, support for 02 years warranty & 03 years AMC	
86.3	Audit & advisory services	Preparation of SRS including one-time infosec audit of MOD-ICG Cloud IT infrastructure, applications as per CERT-IN requirements and other related cyber security standards, preparation of MOD-ICG Cloud specific infosec audit checklist for daily/weekly/monthly for Managed Service Provider (MSP), preparation of CERT-IN specific checklist for biannual audit, by CERT-IN authorised/ empanelled Auditor, One-time payment	
86.4		Quarterly infosec audit as per MOD-ICG Cloud checklist, Biannual infosec audit as per CERT-IN checklist and provide Audit & Advisory Report to onsite MSP for compliance, Recurring payment on bi-annual basis on delivery of services, by CERT-IN authorised/ empanelled Auditor, during warranty & AMC period.	
86.5	VAPT Services	Bidder to ensure minimum 2 runs of VA PT testing for complete implemented solution, including applications, before go-live of the solution. Thereafter, bidder shall conduct VA PT of complete setup once every 6 months during warranty & AMC period. Recommendations and findings of such VA PT tests shall be addressed within stipulated period. The VAPT shall be conducted by a CERT-in impanelled vendor.	

87. **C36 - Edge Cloud Data Rack Specifications**.

HARDWARE SPECIFICATIONS FOR ERP

88. **C37 - All Flash Unified Storage**

Sl.	Parameters	Technical Specification-Unified Storage	Compliance Yes/ No
88.1	Converge/ Unified Storage	Offered Storage array shall be a true converge/ unified storage with a single Microcode/ operating system instead of running different Microcode/ Operating system/ Controllers for File, block and object services respectively.	
88.2	Operating System & Clustering Support	The storage array should support industry-leading Operating System.	
88.3	Capacity & Scalability	(a) The Storage Array shall be offered with all Flash drives in RAID 10 capacity. (b) Storage shall be scalable to minimum of 500TB using 900GB drives.	
88.4	Cache	(a) Offered Storage Array shall be given with Minimum of 48GB cache in a single unit and shall be scalable to 96GB without any controller change. (b) Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache. (c) Offered Storage array shall also have additional support for Flash Cache using SSD/ Flash drives. Both File services as well as Block operations shall be able to utilize flash cache. Minimum of 1TB Flash cache shall be supported. (d) If Flash cache is not supported inside the storage array then vendor shall ensure that offered storage array shall be scalable to minimum of 256GB DRAM cache without any replacement or upgrade of controllers.	
88.5	Processing Power	(a) Offered Storage architecture shall be based on purpose-built ASIC, XOR engine so that there shall be no load on the storage CPU during Raid Parity calculations.	

Sl.	Parameters	Technical Specification-Unified Storage	Compliance Yes/ No
		(b) In case vendor doesn’t have above ASIC functionality then additional 16GB read and write cache shall be provided per controller pair to balance the performance.	
88.6	Architecture & Processing Power	Controllers shall be true active-active so that a single logical unit can be shared across all offered controllers in symmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc.	
88.7	No Single point of Failure	(a) Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc. (b) Minimum of 04 Controllers for redundancy and performance	
88.8	SSD Support	Offered Storage Array shall support 6Gbps dual-ported 1200GB hot-pluggable Enterprise SSD hard drives, Minimum of 400GB SSD/Flash Drives along with support for SSD MDL 1TB /2TB /3TB /4TB drives.	
88.9	SSD Encryption	(a) All SSD should be Self-Encrypted-Drive, FIPS 140-2 Validated (b) All data should be encrypted to ensure Data-in-Rest and required licenses to be included	
88.10	RAID Support & Virtualization	(a) Offered Storage Subsystem shall support RAID 0, 1, 1+0, 5 and RAID 6. (b) Offered storage array shall have native virtualization support so that Raid 1. Raid 5, Raid 1+0, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application. (c) Every supplied disk shall be able to participate into multiple and different raid sets simultaneously. (d) In case vendor doesn't have above functionality, then 20% additional raw capacity shall be provided for each type of disk to balance out the capacity utilization.	
88.11	Data Protection	In case of Power failure, Storage array shall have de-stage feature to avoid any data loss.	
88.12	Protocols	Offered Storage array shall support all well-	

Sl.	Parameters	Technical Specification-Unified Storage	Compliance Yes/ No
		known protocols like FC, ISCSI, FCOE, SMB 3.0, NFS V4, NDMP etc.	
88.13	Host Ports and Back-end Ports	(a) Offered Storage shall have minimum of 4 host ports for connectivity to servers running at 8Gbps speed and shall be scalable to 8 host ports. Offered Storage shall also support: (i) Additional Quad number of 10Gbps ISCSI/ FCOE ports. (ii) Along with ISCSI/ FCOE ports, additional Quad number of 10Gbps IP ports or eight numbers of 1Gbps IP ports for File services operations. (b) Offered storage shall have two additional IP ports for the storage based replication. (c) Offered storage shall have minimum of 16 SAS lanes running at 6Gbps speed and shall be scalable to 32 SAS lanes without any controller change.	
88.14	Global Hot Spare	(a) Offered Storage Array shall support distributed Global Hot Spare for offered SSD/ Flash Disk drives. (b) Global hot spare shall be configure as per industry practice.	
88.15	Performance and Quality of Service	(a) Shall have capability to use more than 30 drives per array group or raid group for better performance. (b) Storage shall be provided with Performance Management Software. (c) Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service/ response time for different application logical units. (d) Quality of service engine shall allow to	

Sl.	Parameters	Technical Specification-Unified Storage	Compliance Yes/ No
		define minimum and maximum cap for required IOPS/ bandwidth for a given logical units of application running at storage array. (e) It shall be possible to change the quality of service Response time, IOPS, bandwidth specification on basis of real time.	
88.16	Thin Provisioning and Space Reclaim	(a) Offered storage array shall be supplied with Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity. (b) Thin Re-claim (Zero Page reclaim) inside storage subsystem shall be automatic in nature and there shall be no need to run any utility inside storage for same. (c) Thin Re-claim inside storage shall not cause any overloading of Storage CPU and shall be able to claim the Zero pages even during peak load without any performance impact (d) For effective capacity utilization, thin reclaim maximum unit shall be 16KB. Vendor shall provide the documentary proof for same. (e) Offered storage array shall be tightly integrated with VMware so that Eager zero disks layout can be used with thin provisioning and thin re-claim.	
88.17	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	
88.18	Snapshot/ Point in time copy/ Clone	(a) Offered Storage shall have support to make the snapshot and full copy (Clone) on the thin volumes if original volume is created on thick or vice-versa. (b) The storage array should have support for both controller-based as well as file system based snapshots functionality (At-least 1024 copies for a given volume or a file store). (c) Storage array shall have functionality to	

Sl.	Parameters	Technical Specification-Unified Storage	Compliance Yes/ No
		re-claim the space from Thin Provisioned Deleted snapshot automatically. Vendors shall provision at-least 20% additional space over and above the actual requirements, if space re-claim from thin provisioned deleted snapshot is not possible automatically.	
88.19	Quota Management and Antivirus Scanning	(a) For file services operations, offered storage shall support both user level as well as file level hard and soft quota. (b) For file services operations, offered storage shall support integration with industry leading antivirus vendors like Symantec and MacAfee.	
88.20	Storage Array Configuration & Management Software	(a) Vendor shall provide Storage Array configuration and Management software. (b) Software shall be able to manage more than one array of same family.	
88.21	Storage Tiering	(a) Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online. (b) For effective data tiering, Storage subsystem shall support automatically Policy based Sub-LUN Data Migration from one Set of drive Tier to another set of drive tier.	
88.22	Remote Replication	(a) The Storage array shall also provide three ways (3 Data Centres) replication to ensure zero RPO in native fashion without using any additional replication appliance. (b) Replication shall support incremental replication after resumption from Link Failure or failback situations.	

89. **C38-Tape Library**

Sl.	Technical Specifications – Tape Library	Compliance Yes/ No
89.1	Offered Tape Library shall support Native data capacity of minimum of 280TB (uncompressed) expandable to minimum of	

Sl.	Technical Specifications – Tape Library	Compliance Yes/ No
	700TB (2.5:1 compressed) using LTO-7 Technology.	
89.2	Tape Library shall provide web based remote monitoring capability.	
89.3	The Tape Library unit shall be configured with 4 FC LTO Gen-7 Tape Drives.	
89.4	Tape Library shall be scalable to four FC LTO-7 drives within the same frame.	
89.5	Offered tape library shall be offered with minimum of 48 Cartridge slots and barcode reader	
89.6	Tape Drive Architecture in the Library shall conform to INCITS/T10 SCSI-3 standard or newer standards.	
89.7	Offered LTO-7 drive in the library shall conform to the Data rate matching technique for higher reliability.	
89.8	Offered LTO-7 drive in the library shall offer optional WORM support and embedded AES 256 bit encryption.	
89.9	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.	
89.10	Offered LTO-7 drive shall have native speed of 300MB/sec.	
89.11	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.	
89.12	Tape Library shall provide native Fiber connectivity to SAN Environment.	
89.13	For optimal Performance. Tape Library shall provide native 8Gbps FC interface connectivity to SAN switches.	
89.14	Tape Library shall be offered with minimum of 48 slots and barcode reader.	
89.15	Tape library shall support removable magazine and mail slot.	
89.16	Tape Library shall have GUI Front panel.	
89.17	Tape Library shall have option for redundant power supply.	
89.18	Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.	
89.19	Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.	

90. **C39- Composable IT Infrastructure with SDDC**

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.1	**General Requirements**	**Composable IT Infrastructure**	
90.2	Fluid resource pool	Disaggregated resource control to enable ability to independently scale resources including memory, storage and compute	
90.3		Compute, storage and networking resources should be fluid, separated from underlying physical infrastructure and independent of each other	
90.4		Proposed solution should support heterogeneous platforms, hypervisors and next generation containers and Bare metal servers concurrently on the same cluster	
90.5		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	
90.6		Should provide unified single GUI to manage fluid resource pool	
90.7	Scalability	Proposed solution should be scalable upto 1000 nodes in a single cluster	
90.8		Linear scalability of IT resources	
90.9	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	
90.10		Enables developers to programmatically deploy new virtual machines and other structures so that they can more quickly test their code	
90.11		Allows an application to automatically instantiate new infrastructure based on performance conditions at the present time	
90.12		Enables automation-based user self-service, and provide 'Private Cloud' services	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.13		Support DevOps	
90.14	OEM ERP Certification	Should be certified for deployment by OEM of ERP being offered to ICG	
90.15	SDDC Support	Should support Software Defined Data Centre (SDDC), detailed requirements are as defined in succeeding specifications	
90.16		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	
90.17	Support	Hardware and Software support to be from the same, single OEM and not outsourced from any third party, either licensed or non-licensed	
90.18	Performance	Proposed solution should be capable of providing 2,00,000 IOPS per node in the environment	
90.19		Solution should be able to provide under 2 millisecond latency	
90.20		80TB Backup should be completed in 8 hour window	
90.21		The proposed solution should support NVMe SSD disks	
90.22		The proposed solution should support 500GB or more of memory per node	
90.23		The proposed solution should support SIX 9's of High Availability	
90.24	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	
90.25		Proposed solution should have the ability to scale compute and storage together or individually in the same cluster	
90.26		Proposed solution should optimize the storage capacity consumption without creating independent workload islands within a single cluster	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.27		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	
90.28		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	
90.29		Should support the Dial home feature to proactively alert of failures	
90.30		The solution should support the seamless upgrade of storage controller capabilities and storage	
90.31		The solution should allow common management across storage tiers. It should support the migration of volumes between storage tiers	
90.32		Software defined storage fault domains provide the ability to tolerate rack failures in addition to disk, network and host failures.	
90.33		Solution should support an all-flash architecture delivering consistent, predictable performance with sub-millisecond response times with appropriate disks/ SSDs.	
90.34		Provider REST API interface to enable the automation of operations through an external management tool	
90.35	Compute Node	(a) 2 socket x 20 Core, 2.0 GHz per Node or latest (b) Intel Xeon Gen10 or latest (c) Processor cache 38 MB or higher (d) DDR4-2666 NVDIMM or higher (d) NVMe SSD, 12 G or higher (e) Memory should feature Advanced ECC, Memory Mirroring Mode and Memory Sparing (f) Silicon Root-of-Trust inbuilt into System-on-Chip (g) Overall sizing should meet or exceed recommendations of ERP OEM	

Sl.	**Parameters**	**Technical Requirements for Composable IT Infrastructure**	**Compliance Yes/ No**
92.36	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 SAS HDD	
2.0.0	**SDDC-Native Cloud**	**Composable IT Infrastructure**	
90.37	Automation & Provisioning	The solution should be able to automate and provision data-Centre services such as compute, storage, networking, backup, replication, load balancing, fault tolerance, security, firewall, etc.	
90.38	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	
90.39	In-built HA	Cloud solution components should have inbuilt High-Availability(HA) functionality without any dependency for all integral elements	
90.40	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	
90.41	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.	
90.42	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	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.43	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	
90.44	Log analysis	The solution should be able capture events and logs from 3rd party sources like servers, storage, OS, 4Applications near real time to perform log analysis and provide out of box dashboards for time series based log analysis	
90.45	OpenStack Integration	Shall natively integrate with 'Enterprise OpenStack' and support multiple hypervisors of VMware ESXi, Microsoft Hyper-V , Oracle VM, Xenserver and KVM	
3.0.0	**SDDC-Virtualisation**	**Composable IT Infrastructure**	
90.46	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	
90.47	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)	
90.48	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.	
90.49	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	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
		Operating System Clustering and should work with FC/ iSCSI SAN and NAS shared storage.	
90.50	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.	
90.51	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	
90.52	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.	
4.0.0	**SDDC - Network Virtualisation**	**Composable IT Infrastructure,**	
90.53	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.	
90.54	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.	
90.55	Live migration of security policies	The Security policies must follow the VM in the event of migration (i.e. live migration)	
90.56	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.	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.57	Native integration with 3rd party security solutions	The solution should offer to Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services.	
90.58	Network Function Virtualisation (NFV)	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 Desktop Infrastructure without the need for complex VLANs, ACLs, or hardware configuration syntax on physical network.	
90.59	Link encryption	The solution should provide Industry-standard IPsec and SSL VPN capabilities that enables securely extending the virtual datacentre. This Site-to-site VPN support would link virtual datacentres and enable hybrid cloud computing at low cost. The SSL VPN capability would deliver remote administration into the virtual datacentre through a bastion host, the method that is favoured by auditors and compliance regulators.	
90.60	Clustering across data Centre	The solution should enable technology for network virtualization, providing network abstraction, elasticity and scale across the datacentre. It should provide technology to scale applications across clusters and pods without any physical network reconfiguration	
5.0.0	**SDDC - Compute Virtualisation**	**Composable IT infrastructure**	
90.61	Compute requirement	(a) The compute configured should have minimum Spec Int Ratings Base 1760 - CPU2006 or better (b) Each compute node should deliver minimum 75000 SAP Count/ equivalent at 65% CPU Utilization or equivalent	
90.62	Data Protection	Compute node should have dedicated cache in raid controller for data protection	
90.63	Power Supply	High-efficiency, hot-plug, Platinum Efficient redundant power supplies	

Sl.	Parameters	Technical Requirements for Composable IT Infrastructure	Compliance Yes/ No
90.64	OS Support	(a) Microsoft Windows Server 2016 Standard/Data Centre Edition (b) Novell SUSE Linux Enterprise Server (c) Red Hat Enterprise Linux	
90.65	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	
90.66	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	

91. **C40-Software Defined Data Centre (SDDC) for DC, DR & ROBO sites**

Sl.	Parameters	Technical Specification-SDDC for DC, DR & ROBO	Compliance Yes/ No
91.1	**Key SDDC requirements**	Should provide Software Defined Compute, Storage and Networking	
91.2		Should provide **automation & orchestration** and support self-service for provisioning/ de provisioning of Compute/ storage/ networking on-the-fly	
91.3		Enterprise wide utilization **'Single-pane-of-monitoring and management**' from single integrated window	
91.4		**High-Availability** (HA) configuration with no 'Single-point-of-failure'	
Software Defined Compute			
91.5	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	

Sl.	Parameters	Technical Specification-SDDC for DC, DR & ROBO	Compliance Yes/ No
91.6		Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS	
91.7	Multi-OS support	Virtualization software shall allow heterogeneous support for guest Operating systems.	
91.8	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.	
91.9	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	
91.10	OpenStack API integration	Virtualization solution should have the capability to provide out of box integration with Open stack API's and should support all services of Core Open Stack	
91.11	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.	
Software Defined Storage			
91.12	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	
91.13		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.	
91.14	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	

Sl.	Parameters	Technical Specification-SDDC for DC, DR & ROBO	Compliance Yes/ No
91.15	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	
91.16	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.	
91.17	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 appliance.	
Software Defined Networking			
91.18	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.	
91.19		The Solution should offer Centrally managed distributed L2-L4 stateful firewall that is kernel-level integrated into the host architecture	
91.20	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.	
91.21	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	
91.22	Security policy affinity	The Security policies must follow the VM in the event of migration (i.e. live migration)	

VERIFIED

Sl.	Parameters	Technical Specification-SDDC for DC, DR & ROBO	Compliance Yes/ No
91.23	SD-WAN integration	Should integrate natively with SD-WAN software for ICG	
SDDC – Automation and Orchestration			
91.24	Self-service	Provide Self-service portal for Users to enable provisioning/ de-provisioning of Computer, Storage and Networking on-demand	
91.25		Should provide PaaS, IaaS services across IT resources on ICG DC, DR and ROBO sites	
91.26	Application Delivery	Automate application delivery and container management	
91.27	SSO support	Should support Single-Sign-On	
91.28	What-if analysis	Provide What-if analysis for various Orchestration related situations	
SDDC – Operations			
91.29	DevOps support	Should support DevOps	
91.30	Container support	Should natively support Containers of Docker/ Kubernetes	
91.31		Provision/ deprovisioning of Containers in native utilization on environment	
91.32		Provide HA support for Containers	
91.33		Provide persistent storage across Containers	
91.34		Support micro-segmentation for Containers	
91.35		Provide dedicated Container management portal integrated into SDDC main console	
91.36		Provide Docker image repository	
91.37	Performance & Capacity Monitoring Dashboard	Should provide Performance monitoring and analysis on SDDC capacity utilization	
91.38		Should provide aggregated compute/ storage utilization analysis at cluster, site and enterprise level	
91.39		Should provide real-time predictive capacity management including trending, metering, right-sizing, optimization to achieve enhanced utilization of IT resource	

Sl.	Parameters	Technical Specification-SDDC for DC, DR & ROBO	Compliance Yes/ No
91.40		Monitoring of OS Resources including CPU, disk, memory, network etc.	
91.41	Overall cost view	Should provide overall cost associated with provisioned IT resources such as VM, Storage etc.	
91.42	What-if analysis	Provide What-if analysis for various operations related situations	
91.43	Application Monitoring	Should able to monitor Application, Middleware and Database for leading enterprise software systems	
91.44		Should natively support application monitoring for Oracle Fusion Middleware, Oracle Databased, Cisco CUCM for Enterprise Unified Communication and MS Exchange.	

92. **C41-Backup, Recovery & Replication for Business Continuity.**

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
92.1	High Availability	No Single-Point-of-Failure architecture and associated components should be provided	
92.2		The solution should support VM on HA configuration	
92.3	Licensing	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.	
92.4	Application awareness	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.	

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
92.5	Hardware Agnostic	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.	
92.6	Granular recovery	Backup software should support file level recovery from an image level backup of Windows\Linux guest file systems.	
92.7		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.	
92.8	VM replication	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 network addresses at the destination site.	
92.9	Unified console operation	Backup software should provide Backup and Replication capabilities in one console only.	
92.10	Encryption, WAN optimization	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.	
92.11		The proposed backup solution must support at least AES 256-bit encryption capabilities for Data-in-Rest, Data-in-Transfer support	
92.12	Tape library	Should support tape mirroring of the same job running concurrently with primary backup.	
92.13		Should allow creating tape clone facility after the backup process.	
92.14	Recovery verification	Backup software must have a feature of data validation, whereby a workload is powered-on in a sandbox environment and tested for its	

Sl.	Category	Technical Requirements – Backup, Recovery & Replication	Compliance Yes/ No
		recoverability.	
92.15		Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency.	
92.16	API Integration	Should provide RESTful API for integration with 3rd party Enterprise applications	
92.17	Unified management console	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.	
92.18	Replication on offline connectivity	Should support auto ROBO replication with central site on restoration of network without any manual intervention	
92.19		Recovery of ROBO sites from central backup at data centre should be supported with zero-touch at ROBO. Take backup of ROBO sites locally and then replicate it to central location	

93. **C42 - Application Delivery Controller (ADC)**

Sl.	Parameters	ADC - Technical Requirements	Compliance Yes/ No
93.1	Platform	It should be a full proxy architecture and must perform reverse proxy for inside applications	
93.2		Should have full support IPv6. It should support all IPv6 scenarios: (a) IPv4 on the inside and IPv6 on the outside (b) IPv6 on the inside and IPv4 on the outside (c) IPv6 on the inside and outside	
93.3		Should support VLAN, LACP & Trunking	
93.4		Appliance should support minimum throughput of 3 Gbps	
93.5		The solution must support to Server Load Balancing along with protection from web based attacks	

Sl.	Parameters	ADC - Technical Requirements	Compliance Yes/ No
93.6		Should have an option to offload SSL functionality to a dedicated hardware/ Appliance of same OEM	
2.0	Performance	Should support upto 60 Gbps as scalability factor and should be provisioned with 03 Gbps. Throughput at L7.	
93.7		Should have capability to support up to 10 Million Concurrent Connections	
93.8		Should have 3400 TPS, where TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate	
93.9		Should have 18000 SSL TPS, using a ECC SSL Certificate	
93.10		Should have compression throughput of minimum 2.7 Gbps	
93.11		Should support configurable TCP/IP queuing and buffering	
3.0	Server Load Balancing	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, based SSL offload and server side compression	
93.12		Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts	
93.13		Should be able to tune monitoring frequency and time automatically when server is available for long time, this is to avoid monitoring load on server	
93.14		Should have 2048 and 4096 bit key for SSL certificate support	
93.15		Should have capability to support ECC, RSA and ECC+RSA (Hybrid) Certificates for SSL offload	
93.16		Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive	

VERIFIED

Sl.	Parameters	ADC - Technical Requirements	Compliance Yes/ No
		and observed	
93.17		Should be application aware and provide Full Proxy for protocols such as HTTP, HTTPS, FTP, SIP, DNS, Diameter, RADIUS etc.	
93.18		Should support inspection of SSL traffic for reverse proxy and forward proxy deployment. Should also support ICAP interface for integration with external security systems.	
93.19		Should support IoT Device authentication over SSL and MQTT Message parsing and MQTT load balancing.	
93.20		Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1	
4.0	Security	Should be an ICSA certified	
93.21		WAF should have positive and negative security model and also perform application layer encryption to protect user identity.	
93.22		The proposed WAF should be equipped with a set of pre-built application specific security policies that provide out-of-the-box protection for common applications	
93.23		The proposed solution should have a dynamic policy builder engine, which is responsible for automatic self-learning and creation of security policies. It should automatically build and manage security policies around newly discovered vulnerabilities without manual intervention.	
93.24		The proposed solution should defend against the OWASP Top 10 Vulnerabilities	
93.25		It should have capability to automatically analyse attacks like Brute Force and avail CAPTCHA on the fly to users to identify bot / scripted attacks	
93.26		It should have Proactive BOT defence and must have BOT signatures	

Sl.	Parameters	ADC - Technical Requirements	Compliance Yes/ No
93.27		It must be able to detect the presence of Remote Access Trojans (RATs) residing in the user's web browser.	
93.28		It should perform comprehensive countermeasure to protect against zero day attack, Challenge – Response Mechanism, which should be able to detect and protect attacks in real time through inbuilt Captcha Mechanism	
93.29		It should encrypt the sensitive field in the application in real time as compared to being encrypted after a submit button or equivalent being pressed	
93.30		It should be able to protect Cookie Poisoning and Cookie Tampering.	
93.31		Should support signature staging after update – so that newly added signature to a policy in block mode does not break the application. If needed this can be disabled.	
5.0	Device Administration	Should provide HTTPS interface management for administering the device	
93.32		Should provide SSH interface management for administering the device	
93.33		Should provide troubleshooting and traffic analysis tool like tcp dump	
93.34		Should support role based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator	
93.35		Should have a built-in tool to take a snapshot of the unit for troubleshooting and analysis purpose	
93.36		Vendor should provide a service to upload this snapshot and get feedback on the health of the unit & missing Hotfixes and best practices	
6.0	High Availability	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL ID mirroring. Hence old connection should not fail or forced for	

Sl.	**Parameters**	**ADC - Technical Requirements**	**Compliance Yes/ No**
		SSL renegotiation.	
93.37		Should have transparent failover between 2 devices, the failover should be transparent to other networking devices	
93.38		Should support network based failover for session mirroring, connection mirroring and heartbeat check	
93.39		Should support config auto sync, manual sync to and from active and backup unit	
93.40		Should support the feature to force the active device to standby and back to active state; or force a device to offline mode	
7.0	Reporting Features	Should have a Reporting Engine built-in	
93.41		Should support High Speed Logging to a syslog server	
93.42		Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc.	
93.43		Should have a log publisher to publish logs to multiple log destinations for the same application (or virtual server)	
93.44		Should have a filtering capability before publishing to a log destination	
8.0	Others	OEM should be listed in Gartner leader quadrant for ADC for last 3 years consecutively	
93.45		Bidder may provide combination of products or integration with 3rd party products as turn-key solution to meet Buyer requirement. However, such integration/ combinations should be validated/ certified respective OEMs for support.	

94. **C43 - Rack Server**

Sl.	Category	Technical Requirements for Rack Server	Compliance Yes/ No
94.1	Compute	(a) 2 socket x 18 Core, 3.0 GHz per Node (b) Intel Xeon Gen9 or latest (c) Processor cache 25 MB or higher (d) 1024 GB DDR4-2666 NVDIMM or higher (d) Minimum SSD 2x250GB, 12 G (e) Memory should feature Advanced ECC, Memory Mirroring Mode and adaptive double device data correction / Memory Online Spare	
94.2	Storage	(a) Support minimum of 04 SFF 12G SAS/ 6G SSD (b) Capacity to be scalable upto 100 TB or higher per node	
94.3	Network	(a) Provide FC-HBA in High Availability with SAN Switch (b) Provide Ethernet ports in HA as required	
94.4	Other Software	(a) Windows 2016 Server DC Edition or latest with SA (b) Backup software, 10 VM or 02 Socket (c) Endpoint Protection Software - 01 No. (d) Virtualisation software – 02 Socket	

95. **C44-ROBO Servers**.

Sl.	ROBO Technical Requirements	Value	Compliance Yes/ No
95.1	**Compute Infra**		
95.2	Ruggedised Hyper Converged Appliance	Yes	
95.3	Min. Processor Sockets per Node	Dual	
95.4	Compute Nodes	3	
95.5	Quorum Node	1	
95.6	Min. Core per Processor	16 or more	
95.7	Min. Processor Speed	2.1 Ghz or better	
95.8	Min. RAM per Node excluding overhead memory for HCA, Virtualisation, Network etc.	1 TB or more	
95.9	During system boots, the system's software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified	Yes	
95.10	Advanced ECC for RAM	Yes	
95.11	Storage Media	SSD	

VERIFIED

Sl.	ROBO Technical Requirements	Value	Compliance Yes/ No
95.12	Storage Available Capacity, 2RF	4 TB or more	
95.13	Storage Scalability	20 TB or more	
95.14	L3 Switch, SDN Ready	Yes	
95.15	SRST support for IPPBX	Yes	
95.16	SRST in-built/ external	Either	
95.17	Min. Switch Speed	10 Gbps or more	
95.18	Switch Redundancy	Active-Active	
95.19	Link Load Balancer, Virtual	Yes	
95.20	WAN Link Optimiser	Yes	
95.21	WAN bandwidth monitoring	Yes	
95.22	EAL/NDPP certified	Yes	
95.23	Support for OSPF, VRRP, 1588v2, SNMPv3	Yes	
95.24	Support for security features of IEEE 802.1ae 256-bits encryption, TACACS, RADIUS, 802.1x, RADIUS Change of Authorization, Dynamic VLAN, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard	Yes	
95.25	Rugged Enclosure, MIL Grade	Yes	
95.26	Marine grade installation	Yes	
95.27	Rail mounted rack for space optimisation on Ships	Yes	
95.28	HCA OEM inter-operability certification for Server, Storage, Network components	Yes	
95.29	OEM certified Inter-operability with existing Central Cloud Management Software VMware vCentre, vROps(Required licenses be provisioned)	Yes	
95.30	OEM certified Inter-operability, log compatibility for all SIEM products as mentioned in latest Gartner Magic Quadrant for SIEM	Yes	
95.31	WAN optimised	Yes	
95.32	Local store and forward of event logs, monitoring data for WAN bandwidth optimisation	Yes	
95.33	OEM benchmarked control, management traffic be provided	Yes	
95.34	WAN latency support up to	200ms	
95.35	High Availability for Compute, Network, Power	Yes	

Sl.	ROBO Technical Requirements	Value	Compliance Yes/ No
95.36	Local, Remote backup support, WAN optimised	16 VM	
95.37	Bare metal, File Backup, WAN optimised	2 Node	
95.38	Site recovery over WAN	Yes	
95.39	Lights-Out Management	Yes	
95.40	internal hot-swappable Redundant Power supply	Yes	
95.41	Rack Type	Integrated Containment	
95.42	IT Power	3.5 kW	
95.43	Usable rack space maximum	42U	
95.44	Redundant separate raw power supply & distribution units within data rack	Yes	
95.45	Precision Cooling with EC Fan ,bottom to top discharge ,Washable filter with minimum 80% efficiency and HDPE media	Yes	
95.46	Redundant Condenser	Yes	
95.47	Condenser Location	External	
95.48	Emergency Cooling Fan	No	
95.49	Variable Speed Scroll Compressor	Yes	
95.50	Anticorrosive Condenser coil for coastal area environmental application	Yes	
95.51	UPS Location	Internal	
95.52	UPS Battery Type	SMF	
95.53	UPS Battery Location	External	
95.54	Battery Backup, 90% load	15 Min or more	
95.55	UPS Redundancy	Yes	
95.56	UPS Battery Redundancy	N+2	
95.57	Central NOC Monitoring, Single-Pane-of-Glass (SPOG)	Yes	
95.58	Multi-brand, Vendor neutral, Open-Architecture/ Protocol supported for Central NOC Monitoring	Yes	
95.59	IP PDU(Vertical , Single Phase)	Yes	
95.60	Environment temperature monitoring	Yes	
95.61	Raw power, regulated power monitoring	Yes	
95.62	Humidity monitoring	Yes	
95.63	UPS battery health, capacity monitoring	Yes	
95.64	Smoke, Fire Detection monitoring	Yes	
95.65	Door opening monitoring	Yes	
95.66	SNMP enabled for all parameters mentioned for monitoring	Yes	

Sl.	ROBO Technical Requirements	Value	Compliance Yes/ No
95.67	Vibration monitoring	No	
95.68	Group ROBO units into logical, hierarchical for management flexibility, AD integrated for Organisation Unit	Yes	
95.69	Support for SNMP, MQTT Protocols	Yes	
95.70	Compressor running hours monitoring	Yes	
95.71	Central monitoring software should support virtual appliance	Yes	
95.72	Support offline monitoring data, log store & forward for Ships and ROBO	Preferred	
95.73	Smoke and Fire Detection	Yes	
95.74	Fire Suppression	No	
95.75	Rodent Repellent, Ultra Sonic	Yes	
95.76	Water leak detection	Yes	
95.77	WAN optimised	Yes	
95.78	Local store and forward of event logs, monitoring data for WAN bandwidth optimisation	Yes	
95.79	OEM benchmarked control, management traffic be provided	Yes	
95.80	WAN latency support up to	200ms	
95.81	laying of appropriate power cabling from Main panel to rack up to 50mtrs, required MCB, Electrical accessories along with Chemical earthing	Yes	
95.82	Biometric Access Control, AD integrated	Yes	
95.83	Minimum of 04 out of 05 ROBO components of data rack including, Ventilation/ Cooling, UPS, IP-PDU, integrated Data Rack enclosure and centralised monitoring software similar to DCIM should be of same single OEM to have seamless integration and management support	Yes	

96. **Miscellaneous**

Sl.	Specifications	Value	Compliance Yes/ No
96.1	Redundant MPLS Link	Yes	
96.2	Warranty, 05 Years	Yes	
96.3	Project specific OEM MAF Certificate to System Integrator	Yes	

VERIFIED

96.4	Central NOC Monitoring, Brand agnostic, inter-operable, integrated Single-Pane-of-Glass (SPOG) for Virtualisation, ROBO racks	Yes	
96.5	Min. OEM authorised partners with min. of 05 years of support experience of particular product	Yes	
96.6	OEM Warranty Response time as SLA, All days	4 hrs	
96.7	OEM Warranty Resolution time as SLA, All days	48 hrs	
96.8	Chemical earthing	Yes	
96.9	OEM certified Inter-operability for centralised monitoring and management for all IBMS, NMS, ITOM products as mentioned in latest Gartner Magic Quadrant including leading brands of BMC, Manage Engine	Yes	
96.10	All Central monitoring SPOG software should support virtual appliance form	Yes	
96.11	All active IT systems should support central enterprise Active Directory	Yes	
96.12	Should have OEM 24x7x365 support for hardware/ software in India. Should provide Service Desk contact details and Service Level Agreement (SLA) in proof	Yes	
96.13	All critical components of ROBO Racks like Racks with PDU, UPS, Air Conditioning and Remote Monitoring solution should be from same and single OEM for seamless integration and better after sales service support.	Yes	
96.14	Monitoring of Robo with single pan of glass.	Yes	
96.15	All Robo should be monitor by ICG HQ with single pan of glass.	Yes	

97. **OEM Qualification requirements.** Data Centre, DR Data Centre 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.

TECHNICAL SPECIFICATIONS: NETWORK CONNECTIVITY & COMPONENTS

Introduction

98. Digital India plan of fiber connectivity to all rural Panchayat union offices underlines the importance of network connectivity with adequate bandwidth in digitisation efforts. In similar lines, Digital Coast Guard should interconnect all Coast Guard units including ships using high-speed, highly-secured MPLS (Multiprotocol Label Switching) fiber networking/ VSAT. Equipment to run the Managed MPLS connectivity like Router, Rack, UPS and Earthing needs to be deployed and maintained by Network Bandwidth Service Provider.

99. All CG units need to be connected with high-speed fiber MPLS network from any of the ISP. The SI (System Integrator) should implement the last mile redundant fiber connectivity to CG units including locations such as Jetties.

Design Objectives

100. Main design objectives are as follows: -

100.1 Software-Defined WAN with micro-segmentation using virtual NGFW at all locations including Data Centre, DR DC & ROBO sites.

100.2 Provide highly-scalable, secured, reliable MPLS network connectivity to ICG units including ships at harbour.

100.3 No hardware appliances for routing and security at every remote location as part of 'Software Defined WAN' & 'One Cloud' approach.

100.4 Provide main and protection path to each ICG sites using dark fiber connectivity, wherever feasible.

100.5 Utilise networking security components to ensure data security.

Design Specification

101. Main design specification are as under:-

101.1 Connect ICG units into highly secured MPLS fiber network. ICG units are as per list at para 105 below.

101.2 MPLS links from any of the two different service providers for high-availability.

101.3 Bandwidth requirement of 32 Mbps with compression ratio of 1:1. for MPLS CGWAN units and 1 Gbps for Data Centres. Bandwidth requirement is as per para 105 below.

VERIFIED

101.4 Last mile **main path should be in Under Ground fiber** (minimum required depth of 1.8 mtr) **for Class-'S'** and **'A'**, and protection path should also be fiber. Both Main & Protection path to provide equal band widths.

101.5 Last mile should have both main and protection path for all the location.

101.6 Back bone network should have high end SDH (Synchronous Digital Hierarchy) with MPLS cloud.

101.7 Network should be scalable to 1G/10G or higher.

101.8 Network should be capable of integrating highly secured with IPSec (Internet Protocol Security) encryption suite and other required security mechanisms.

101.9 Routing and security at every remote location as part of 'Software Defined WAN' & 'One Cloud' approach should be through VMs.

101.10 Latest technologies of SD-WAN/ NFV perspective.

101.11 Traffic optimization, resiliency and scalable.

101.12 Branch to branch to IPSEC should be enabled from every remote location to central location.

101.13 Every remote location will have Local LAN connected on basic L3 switches.

101.14 Easy to manage, troubleshoot and operate the network.

101.15 Solution's based on end to end virtualization. High Level Bill of Material

102. High level Bill of Material is as under:-

Sl.	Description	Qty.
102.1	Main path on fiber	As Reqd.
102.2	Protection path on fiber	As Reqd.
102.3	VSAT (Very Small Aperture Terminal) link to Island sites. Link should support mesh topology with 1:1 bandwidth of latency not exceeding 800ms	As Reqd.
102.4	Rugged Hyper-Converged Infrastructure (HCI)/ Hyper-Converged Appliance (HCA) with virtual NGFW for micro-segmentation security. Should provide 100% scale-up & minimum of 2x16+2x16 Cores should be	As Reqd.
102.5	Data Closet, power of minimum 2kW at all ROBO sites	As Reqd.

102.6	Software Defined WAN to provide virtual routing, link load balancing, WAN bandwidth optimisation in HA	As Reqd.
102.7	Centralised management software for ROBO stack including HCI, SD WAN, SD Security stacks	As Reqd.
102.8	L3 switches with SDN in HA	As Reqd.
102.9	Installation, Configuration, three-year support charges	As Reqd.

Note:

(i) All active components should carry minimum 2 years warranty. Core and Access switches and other Brands passive components should carry minimum 2 years warranty.

(ii) All network hardware of router, switch, UTM etc. should be designed to meet scalability of at least 4 times of present bandwidth requirement for each site.

(iii) Generic bill of material is only indicative and of minimum specification only.

103 **List of CG Stations & Designed Bandwidth**.

Class-'S': Link between DC and DR. Bandwidth per link shall be 1 Gbps.

Class-'A': Primary Link of Underground Fiber (UG with minimum depth of 1.8 mtr) and Secondary Link may be UG or Over ground (OG). Bandwidth per link shall be 32 Mbps

Class-'B': Both Primary/ Secondary Links may be OG or UG. Each link should have 32 Mbps bandwidth

Class-'C': Shall be VSAT, 1:1 BW, 2Mbps Uplink, latency not exceeding 800ms

SL	**Link ID**	**Site ID**	**CLASS**	**Site Name**	**Path Type**	**Link Type**	**BW Type**	**BW**
1	L001	S001	A	CGHQ, ICGS(DLI), ICG IDR	P	UG	MPLS	32
2	L002	S001	A	CGHQ, ICGS(DLI), ICG IDR	S	OG	MPLS	32
3	L003	S002	A	CGHQ Annex., Noida Sector-62	P	UG	MPLS	32
4	L004	S002	A	CGHQ Annex., Noida Sector-62	S	OG	MPLS	32
5	L005	S003	B	CGOM (NOI)	P	OG	MPLS	32
6	L006	S003	B	CGOM (NOI)	S	OG	MPLS	32
7	L007	S004	B	CGAOT(KAN)	P	OG	MPLS	32

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
8	L008	S004	B	CGAOT(KAN)	S	OG	MPLS	32
9	L009	S005	B	ICGS (JAK)	P	OG	MPLS	32
10	L010	S005	B	ICGS (JAK)	S	OG	MPLS	32
11	L011	S006	B	ICGS (VDR)	P	OG	MPLS	32
12	L012	S006	B	ICGS (VDR)	S	OG	MPLS	32
13	L013	S007	A	DHQ-15 / ICGS (OKA)	P	UG	MPLS	32
14	L014	S007	A	DHQ-15 / ICGS (OKA)	S	OG	MPLS	32
15	L015	S008	B	CG Jetty, Okha Port Trust	P	OG	MPLS	32
16	L016	S008	B	CG Jetty, Okha Port Trust	S	OG	MPLS	32
17	L017	S009	B	ICGS (VRL)	P	OG	MPLS	32
18	L018	S009	B	ICGS (VRL)	S	OG	MPLS	32
19	L019	S010	A	DHQ-1 , ICGS(PBD)	P	UG	MPLS	32
20	L020	S010	A	DHQ-1 , ICGS(PBD)	S	OG	MPLS	32
21	L021	S011	B	CGAE (PBD), 850 SQN(CG)	P	OG	MPLS	32
22	L022	S011	B	CGAE (PBD), 850 SQN(CG)	S	OG	MPLS	32
23	L023	S012	B	CG Jetty, Porbander Port Trust	P	OG	MPLS	32
24	L024	S012	B	CG Jetty, Porbander Port Trust	S	OG	MPLS	32
25	L025	S013	A	RHQ (NW), ICGS(GDN)	P	UG	MPLS	32
26	L026	S013	A	RHQ (NW), ICGS(GDN)	S	OG	MPLS	32
27	L027	S014	B	ICGS (MDR)	P	OG	MPLS	32
28	L028	S014	B	ICGS (MDR)	S	OG	MPLS	32
29	L029	S015	B	ICGS (PPV)	P	OG	MPLS	32
30	L030	S015	B	ICGS (PPV)	S	OG	MPLS	32
31	L031	S016	B	CGRPS(SRT)	P	OG	MPLS	32
32	L032	S016	B	CGRPS(SRT)	S	OG	MPLS	32
33	L033	S017	A	ICGAS (DMN)/750,, 841 SQN(CG)	P	UG	MPLS	32
34	L034	S017	A	ICGAS (DMN)/750,, 841 SQN(CG)	S	OG	MPLS	32
35	L035	S018	A	RHQ (W), DHQ-2, ICGS(MBI)	P	UG	MPLS	32
36	L036	S018	A	RHQ (W), DHQ-2, ICGS(MBI)	S	OG	MPLS	32

VERIFIED

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
37	L037	S019	A	Buvik	P	UG	MPLS	32
38	L038	S019	A	Buvik	S	OG	MPLS	32
39	L039	S020	A	CGSD(MBI)	P	UG	MPLS	32
40	L040	S020	A	CGSD(MBI)	S	OG	MPLS	32
41	L041	S107	B	CG Jetty, Indra Dock, Mumbai Port Trust, Mumbai	P	OG	MPLS	32
42	L042	S107	B	CG Jetty, Indra Dock, Mumbai Port Trust, Mumbai	S	OG	MPLS	32
43	L043	S022	B	CGAIS(MBI),842 SQN	P	OG	MPLS	32
44	L044	S022	B	CGAIS(MBI),842 SQN	S	OG	MPLS	32
45	L045	S023	B	ICGS (MJR)	P	OG	MPLS	32
46	L046	S023	B	ICGS (MJR)	S	OG	MPLS	32
47	L047	S024	B	ICGS(RTG)	P	OG	MPLS	32
48	L048	S024	B	ICGS(RTG)	S	OG	MPLS	32
49	L049	S025	B	ICGS (DHU)	P	OG	MPLS	32
50	L050	S025	B	ICGS (DHU)	S	OG	MPLS	32
51	L051	S026	A	DHQ-11/, ICGS (GOA)	P	UG	MPLS	32
52	L052	S026	A	DHQ-11/, ICGS (GOA)	S	OG	MPLS	32
53	L053	S027	A	CGAE (GOA), CGASD(GOA), 800 SQN(CG)	P	UG	MPLS	32
54	L054	S027	A	CGAE (GOA), CGASD(GOA), 800 SQN(CG)	S	OG	MPLS	32
55	L055	S028	B	ICGS (KAR)	P	OG	MPLS	32
56	L056	S028	B	ICGS (KAR)	S	OG	MPLS	32
57	L057	S029	B	CGAOT(BGL)	P	OG	MPLS	32
58	L058	S029	B	CGAOT(BGL)	S	OG	MPLS	32
59	L059	S030	B	CG Jetty, Mangalore Port Trust	P	OG	MPLS	32
60	L060	S030	B	CG Jetty, Mangalore Port Trust	S	OG	MPLS	32

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
61	L061	S031	A	DHQ-3/ ICGS(MNG)	P	UG	MPLS	32
62	L062	S031	A	DHQ-3/ ICGS(MNG)	S	OG	MPLS	32
63	L063	S032	B	ICGS (BPY)	P	OG	MPLS	32
64	L064	S032	B	ICGS (BPY)	S	OG	MPLS	32
65	L065	S033	A	DHQ-4, ICGS Kochi	P	UG	MPLS	32
66	L066	S033	A	DHQ-4, ICGS Kochi	S	OG	MPLS	32
67	L067	S034	A	CGAE(KOC), 747	P	UG	MPLS	32
68	L068	S034	A	CGAE(KOC), 747	S	OG	MPLS	32
69	L069	S035	B	CG Jetty, Naval Dockyard, Kochi	P	OG	MPLS	32
70	L070	S035	B	CG Jetty, Naval Dockyard, Kochi	S	OG	MPLS	32
71	L071	S036	B	ICGS (VZM)	P	OG	MPLS	32
72	L072	S036	B	ICGS (VZM)	S	OG	MPLS	32
73	L073	S037	C	DHQ-12/ ICGS (KAV)	P	VSAT	VSAT	2
74	L074	S038	C	ICGS (MIN)	P	VSAT	VSAT	2
75	L075	S039	C	ICGS (AND)	P	VSAT	VSAT	2
76	L076	S040	A	RHQ(East), MRCC(CHN)	P	UG	MPLS	32
77	L077	S040	A	RHQ(East), MRCC(CHN)	S	OG	MPLS	32
78	L078	S041	A	DHQ-5/ ICGS Chennai	P	UG	MPLS	32
79	L079	S041	A	DHQ-5/ ICGS Chennai	S	OG	MPLS	32
80	L080	S042	B	BMU(CHN)	P	OG	MPLS	32
81	L081	S042	B	BMU(CHN)	S	OG	MPLS	32
82	L082	S043	A	CGSD(CHN)	P	UG	MPLS	32
83	L083	S043	A	CGSD(CHN)	S	OG	MPLS	32
84	L084	S044	A	CGAS(CHN), CGAIS(CHN), 744 SQN(CG), 848 SQN(CG)	P	UG	MPLS	32
85	L085	S044	A	CGAS(CHN), CGAIS(CHN), 744 SQN(CG), 848 SQN(CG)	S	OG	MPLS	32
86	L086	S045	B	CG Jetty, Chennai Port Trust, Chennai	P	OG	MPLS	32

VERIFIED

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
87	L087	S045	B	CG Jetty, Chennai Port Trust, Chennai	S	OG	MPLS	32
88	L088	S046	B	ICGS (MDP)	P	OG	MPLS	32
89	L089	S046	B	ICGS (MDP)	S	OG	MPLS	32
90	L090	S047	B	ICGS (TUT)	P	OG	MPLS	32
91	L091	S047	B	ICGS (TUT)	S	OG	MPLS	32
92	L092	S048	B	CG Jetty, Tuticorin Port Trust	P	OG	MPLS	32
93	L093	S048	B	CG Jetty, Tuticorin Port Trust	S	OG	MPLS	32
94	L094	S049	B	ICGS(KKL)	P	OG	MPLS	32
95	L095	S049	B	ICGS(KKL)	S	OG	MPLS	32
96	L096	S050	A	DHQ-13/ ICGS (PCY)	P	UG	MPLS	32
97	L097	S050	A	DHQ-13/ ICGS (PCY)	S	OG	MPLS	32
98	L098	S051	A	DHQ-6/ ICGS (VZG)	P	UG	MPLS	32
99	L099	S051	A	DHQ-6/ ICGS (VZG)	S	OG	MPLS	32
100	L100	S052	B	CG Jetty, Naval Dockyard, Vizag	P	OG	MPLS	32
101	L101	S052	B	CG Jetty, Naval Dockyard, Vizag	S	OG	MPLS	32
102	L102	S053	B	ICGS(KPM)	P	OG	MPLS	32
103	L103	S053	B	ICGS (KPM)	S	OG	MPLS	32
104	L104	S054	B	ICGS(NPM)	P	OG	MPLS	32
105	L105	S054	B	ICGS(NPM)	S	OG	MPLS	32
106	L106	S055	B	CG Jetty, Kakinada Port Trust - Rajdhwaj, (F-1)	P	OG	MPLS	32
107	L107	S055	B	CG Jetty, Kakinada Port Trust - Rajdhwaj, (F-1)	S	OG	MPLS	32
108	L108	S056	B	ICGS (KND)	P	OG	MPLS	32
109	L109	S056	B	ICGS (KND)	S	OG	MPLS	32
110	L110	S057	A	DHQ-7/ ICGS (PDP)	P	UG	MPLS	32
111	L111	S057	A	DHQ-7/ ICGS (PDP)	S	OG	MPLS	32
112	L112	S058	A	CGSD(PDP)	P	UG	MPLS	32
113	L113	S058	A	CGSD(PDP)	S	OG	MPLS	32

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
114	L114	S059	B	CG Jetty, Paradip Port Trust	P	OG	MPLS	32
115	L115	S059	B	CG Jetty, Paradip Port Trust	S	OG	MPLS	32
116	L116	S060	B	ICGS (GPR)	P	OG	MPLS	32
117	L117	S060	B	ICGS (GPR)	S	OG	MPLS	32
118	L118	S061	A	CGAE(BVR)	P	UG	MPLS	32
119	L119	S061	A	CGAE(BVR)	S	OG	MPLS	32
120	L120	S062	A	RHQ(NE), ICGS (KOL)	P	UG	MPLS	32
121	L121	S062	A	RHQ(NE), ICGS (KOL)	S	OG	MPLS	32
122	L122	S063	B	700 SQN(CG)	P	OG	MPLS	32
123	L123	S063	B	700 SQN(CG)	S	OG	MPLS	32
124	L124	S064	A	DHQ-8/ ICGS (HLD)	P	UG	MPLS	32
125	L125	S064	A	DHQ-8/ ICGS (HLD)	S	OG	MPLS	32
126	L126	S065	B	CG Jetty, Haldia Port	P	OG	MPLS	32
127	L127	S065	B	CG Jetty, Haldia Port	S	OG	MPLS	32
128	L128	S066	B	ICGS (FZR)	P	OG	MPLS	32
129	L129	S066	B	ICGS (FZR)	S	OG	MPLS	32
130	L130	S067	B	CGTLO(BKP)	P	OG	MPLS	32
131	L131	S067	B	CGTLO(BKP)	S	OG	MPLS	32
132	L132	S068	B	CG Jetty, Port Blair	P	OG	MPLS	32
133	L133	S068	B	CG Jetty, Port Blair	S	OG	MPLS	32
134	L134	S069	A	RHQ(A&N)/, DHQ-14/ ICGS(PBR)	P	UG	MPLS	32
135	L135	S069	A	RHQ(A&N)/, DHQ-14/ ICGS(PBR)	S	OG	MPLS	32
136	L136	S070	B	RSD (PBR)	P	OG	MPLG	32
137	L137	S070	B	RSD (PBR)	S	OG	MPLG	32
138	L138	S071	B	745 SQN(CG), CGAE PORTBLAIR	P	OG	MPLS	32
139	L139	S071	B	745 SQN(CG), CGAE PORTBLAIR	S	OG	MPLS	32
140	L140	S072	C	DHQ-9/ ICGS (DGP)	P	VSAT	VSAT	2
141	L141	S073	C	DHQ-10/ ICGS (CBL)	P	VSAT	VSAT	2
142	L142	S074	C	ICGS (MYB)	P	VSAT	VSAT	2

VERIFIED

SL	**Link ID**	**Site ID**	**CLASS**	**Site Name**	**Path Type**	**Link Type**	**BW Type**	**BW**
143	L143	S075	C	ICGS(KAM)	P	VSAT	VSAT	2
144	L144	S076	C	ICGS(HBY)	P	VSAT	VSAT	2
145	L145	S077	A	CGSD (Kochi)	P	UG	MPLS	32
146	L146	S077	A	CGSD (Kochi)	S	OG	MPLS	32
147	L147	S078	A	CGDA	P	UG	MPLS	32
148	L148	S078	A	CGDA	S	OG	MPLS	32
149	L149	S079	B	PCDA	P	OG	MPLS	32
150	L150	S079	B	PCDA	S	OG	MPLS	32
151	L151	S080	B	CDA(Delhi)	P	OG	MPLS	32
152	L152	S080	B	CDA(Delhi)	S	OG	MPLS	32
153	L153	S081	B	CDA (Kochi)	P	OG	MPLS	32
154	L154	S081	B	CDA (Kochi)	S	OG	MPLS	32
155	L155	S082	B	CDA (Chennai)	P	OG	MPLS	32
156	L156	S082	B	CDA (Chennai)	S	OG	MPLS	32
157	L157	S083	B	CDA (Vizag)	P	OG	MPLS	32
158	L158	S083	B	CDA (Vizag)	S	OG	MPLS	32
159	L159	S084	B	CDA (Kolkatta)	P	OG	MPLS	32
160	L160	S084	B	CDA (Kolkatta)	S	OG	MPLS	32
161	L161	S085	B	CDA (Port Blair)	P	OG	MPLS	32
162	L162	S085	B	CDA (Port Blair)	S	OG	MPLS	32
163	L163	S086	B	CDA (Goa)	P	OG	MPLS	32
164	L164	S086	B	CDA (Goa)	S	OG	MPLS	32
165	L165	S087	B	CDA (Karwar)	P	OG	MPLS	32
166	L166	S087	B	CDA (Karwar)	S	OG	MPLS	32
167	L167	S088	B	Vizag Chetak Flight	P	OG	MPLS	32
168	L168	S088	B	Vizag Chetak Flight	S	OG	MPLS	32
169	L169	S089	B	CGRPT (Vizag)	P	OG	MPLS	32
170	L170	S089	B	CGRPT (Vizag)	S	OG	MPLS	32
171	L171	S090	B	CGRPT (Kolkata)	P	OG	MPLS	32
172	L172	S090	B	CGRPT (Kolkata)	S	OG	MPLS	32
173	L173	S091	B	CGRPT (Goa)	P	OG	MPLS	32
174	L174	S091	B	CGRPT (Goa)	S	OG	MPLS	32

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
175	L175	S092	B	CGRPT (Kochi)	P	OG	MPLS	32
176	L176	S092	B	CGRPT (Kochi)	S	OG	MPLS	32
177	L177	S093	B	CGRPT (Chennai)	P	OG	MPLS	32
178	L178	S093	B	CGRPT (Chennai)	S	OG	MPLS	32
179	L179	S094	B	CGRPT (Pipav)	P	OG	MPLS	32
180	L180	S094	B	CGRPT (Pipav)	S	OG	MPLS	32
181	L181	S095	B	PRT (West)	P	OG	MPLS	32
182	L182	S095	B	PRT (West)	S	OG	MPLS	32
183	L183	S096	B	PRT (East)	P	OG	MPLS	32
184	L184	S096	B	PRT (East)	S	OG	MPLS	32
185	L185	S098	A	CGSD (PBD)	P	UG	MPLS	32
186	L186	S098	A	CGSD (PBD)	S	OG	MPLS	32
187	L187	S099	B	ACV 73 SQN	P	OG	MPLS	32
188	L188	S099	B	ACV 73 SQN	S	OG	MPLS	32
189	L189	S100	B	CG Jetty, Murmugoa Port Trust	P	OG	MPLS	32
190	L190	S100	B	CG Jetty, Murmugoa Port Trust	S	OG	MPLS	32
191	L191	S101	S	ICG IDC (MPLS Cloud)	P	UG	MPLS	1000
192	L192	S101	S	ICG IDC (MPLS Cloud)	S	UG	MPLS	1000
193	L193	S097	S	ICG IDC (IDC-DC link)	P	UG	LL	1000
194	L194	S097	S	ICG IDC (IDC-DC link)	S	UG	LL	1000
195	L195	S108	S	CG DR (MPLS Cloud)	P	UG	MPLS	1000
196	L196	S108	S	CG DR (MPLS Cloud)	S	UG	MPLS	1000
197	L197	S021	S	CG DC (MPLS Cloud)	P	UG	MPLS	1000
198	L198	S021	S	CG DC (MPLS Cloud)	S	UG	MPLS	1000
199	L199	S102	S	CG DC (DC-DR link)	P	UG	LL	1000
200	L200	S102	S	CG DC (DC-DR link)	S	UG	LL	1000
201	L201	S109	S	Inter-MPLS-link	P	UG	LL	1000
202	L202	S109	S	Inter-MPLS-link	S	UG	LL	1000
203	L203	S103	B	69 ACV SQN	P	OG	MPLS	32
204	L204	S103	B	69 ACV SQN	S	OG	MPLS	32
205	L205	S104	A	CGAE (MNG)	P	UG	MPLS	32

VERIFIED

SL	Link ID	Site ID	CLASS	Site Name	Path Type	Link Type	BW Type	BW
206	L206	S104	A	CGAE (MNG)	S	OG	MPLS	32
207	L207	S105	B	CGAS (RTI), Ratnagiri	P	OG	MPLS	32
208	L208	S105	B	CGAS (RTI), Ratnagiri	S	OG	MPLS	32
209	L209	S106	B	79 ACV	P	OG	MPLS	32
210	L210	S106	B	79 ACV	S	OG	MPLS	32

104 **Link/Site Summary**

Link/ Site Count	
Links	210
Sites	109
Sites by Class	
Class-S	06
Class-A	30
Class-B	65
Class-C	08
Total Sites	109

FUNCTIONAL REQUIREMENTS - SAFAL ERP

SAFAL ERP-LOGISTICS

Inventory Management & Stores

105 **Introduction.** Inventory management is the process of efficiently Overseeing the constant flow of units into and out of an existing inventory. This process usually involves controlling the transfer in of units in order to prevent the inventory from becoming too high, or diminishing to levels that could put the operation of the organization into jeopardy. Competent inventory management also seeks to control the costs associated with the inventory. Balancing the various tasks of inventory management means paying attention to three key aspects of any inventory. The first aspect has to do with time. In terms of materials acquired for inclusion in the total inventory, this means understanding how long it takes for a supplier to process an order and execute a delivery. Inventory management also demands that a solid understanding of how long it will take for those materials to transfer out of the inventory be established. Knowing these two important lead times makes it possible to know when to place an order and how many units should ordered to keep production running smoothly. Calculating what is known as buffer stock is also key to effective inventory management. Essentially, buffer stock is additional units above and beyond the minimum number required to maintain production levels. For example, the manager may determine that it would be a good idea to keep one or two extra units of a given machine part on hand, just in case an emergency situation arises or one of the units proves to be defective once installed. Creating this cushion or buffer helps to minimize the chance for operations to be interrupted due to a lack of essential parts in the supply inventory. Inventory management is not limited to documenting the delivery of materials and the movement of those materials into operational process. The movement of those materials as they go through the various stages of the operation is also important. Finally, inventory management has to do with keeping accurate records of goods. This often means posting the goods to the inventory totals as well as subtracting the most recent shipments. Accurately maintaining figures on the goods inventory makes it possible to quickly convey information to units as to what is available and ready for shipment at any given time. In addition to maintaining control of the volume and movement of various inventories, inventory management also makes it possible to prepare accurate records that are used for accessing or planning major operations. Without precise data regarding unit volumes within each unit, depot & ship of the overall operation, the organization cannot plan and survive. This could always lead to mismanagement, firefighting & overpaying for resources in the event of emergency.

106 The annual requirements are forecasted based on the past consumption data and future requirements considering the usage and the age of equipment/ machines and appliances for the period under consideration. This includes stores required for maintenance of equipment onboard various class of ships and clothing for service as well as civilian personnel. Based on this forecast, budget will be prepared for the year. For optimal inventory management, the system should managing logistics facilities. The support for inventory management should helps in recording and tracking materials on the basis of both quantity and unique ID. Warehouse inventory management functions should also covers internal warehouse movements and storage, to bring reduction in costs for warehousing, transportation, order fulfilment, and material handling while improving overall services. The application should significantly improves inventory turns, optimize the flow of goods, and shorten routes within the warehouse or distribution Centre. Additional benefits of inventory management should include improved cash flow, visibility, and decision support mechanism.

107 **Key Functional Requirements.**

107.1 Provisioning/Initial Provisioning of Equipment

107.2 Replenishment Provisioning / ARD

107.3 Goods Receipt

107.4 Goods Issue

107.5 Physical Inventory Process - Stock taking

107.6 Survey Stock

Provisioning

108 **Introduction**. The provisioning process, which is the most critical in Indian Coast Guard inventory management, involves activities covering the determining and positioning of equipment, spare parts and stores for providing day to day fleet support, and ship's lifetime maintenance requirements. The provisioning process in the Indian Coast Guard consists of "Initial Provisioning" and "Replenishment Provisioning".

109 **Functional Requirements.**

109.1 System should be able to classify materials as per the business requirement such as Equipment, components, sub components etc.

109.2 System should be able to sort Entitlement/ Authorization unit wise as well as material group wise.

109.3 System should be able to calculate wastage (usage/ consumption) rates (as a percentage of total entitlement) for material groups that are likely to be rendered Beyond Economical Repair or Beyond Local Repair.

109.4 System should be able to take percentage of repairable stock as receipt (sorted material wise).

109.5 System should be able to define custom fields in the planning table as template form for accounting for different figures in the demand and supply side like available stock, stock in transit, maintenance requirements, safety stock requirements, reserve requirements etc.

109.6 System should populate the fields in the planning table based on data/ scales/ authorizations maintained as a part of the table. System should be able to record authorization for each class of ship or for each ship.

109.7 System should be able to alter the quantity of reserves using some algorithm/ calculation running as default in the background. The default algorithms would need to be configured for different reserves based on their end user, degree of indigenization etc.

109.8 System should be able to add, subtract, multiply and divide different fields of the planning table either manually or using some customized algorithm in the back ground.

109.9 System should be able to display the deficits, delayed stock materializations in different color codes.

109.10 System should be able to provide a pre-defined hierarchal approval process to different authorities and enable them to change the figures as per their personal discretion.

109.11 System should be able to raise demands as per following priority:-

109.11.1 O-Operational

109.11.2 N-Normal

109.11.3 U-Urgent

109.12 System should be able to manage Auto replenishment (ARS) on board ships and establishments based on ship wise quarterly/ half yearly allowances and issue to the ships as per its requirement. System to issue part quantity proportionally to all the ships If sufficient quantity of stock not available for a particular ARS item.

109.13 System should be able to issue Non-availability certificate (NAC) against demands for which item is not available in the stock.

109.14 System should be able to check approval of competent authority to raise Prior To Survey (PTS) demand.

109.15 System should be able to check that Replenishment (REP) demands are only raised for consumable items. Refit Demand by Ships/CGRPS and Refit Planning and Progress (RPP) demands should be allowed to be raised only by CG unit/ships.

109.16 System should be to allow planner to close the demand under following circumstances:-

109.16.1 On request of customer

109.16.2 Delivered

109.16.3 Fully complied

109.16.4 Invalid Demand

109.16.5 Multiple Demand

109.16.6 NAC issued

109.16.7 Part complied and closed

109.16.8 Refit completed

109.17 System should be able to roll back the issue if the item has not been released by the Store House staff.

109.18 System should be able to check item authorization to the unit through D-787 or allowance list.

109.19 System should be able to issue all demands on a single click provided if stock available is available.

109.20 System should be able to earmark demands for provisioning and priority issuing.

109.21 Raised in Office (RIO) demands by store depot against items earmarked for units as per the supply order.

109.22 System should able to transfer of items from one store depot to another store depots, if required.

109.23 System should able to generate compliance rates of store depots taking into account the number of demands received, processed, number of items issued and NAC for a given period.

Initial Provisioning of Equipment

110 **Introduction**. The objective of initial provisioning is to "determine", "procure" and "position" spares needed to support equipment for an initial period of 5 years or defined period. These spares, as also, Long Term Exploitation (LTE) spares are known as "Base & Depot" (B&D) spares, and are centrally stocked at Mother Stores Depots. The spares anticipated for consumption during the first year's operational service of a ship, are termed "On Board" (OB) spares, and stored on the ship itself. When consumed, these are replenished from B&D stocks held ashore.

110.1 The process of initial provisioning, thus, has two phases, namely, "determination of requirements" and "acquisition" of these requirements.

110.2 Indian Coast Guard Headquarters is responsible for procurement of initial outfit of B&D spares.

111 **Functional Requirement**.

111.1 System should be able to allow professional directorates to add list of equipment to be fitted on a ship under construction.

111.2 System should be to allow Professional Directorates to add or delete from this list of equipment.

111.3 System should be able to display the available list of equipment to shipyard.

111.4 System should be able to have the capability either directly importing the quote of OEM or uploading from an EXCEL sheet provided by shipyard.

111.5 System should be able to upload or record range and scaling data of spares generated by professional directorates.

111.6 System should be able to classify items into repairable and consumable.

111.7 System should be able to display the details of equipment manufactured by OEM.

111.8 Option for stocking up of stores at store depot of the base port of the ship for the stores whose Transportation cost of spare may be more than the cost of spare.

111.9 On board different class of the ICG ships like FPV and IB class few equipment are in common nature. The System should able to cater for such stores.

Replenishment Provisioning/ ARD

112 **Introduction**. Replenishment provisioning, based on Annual Review of Demands (ARDs), is an ongoing annual exercise for replenishment of stock as per past consumption and future requirements. ARD Projection can be calculated as per following:-

112.1 **Machinery Spares**. Machinery Spares may be calculated as per following:-

(2.5 X D + NAC + Dues-out) - (Stock held + Dues-in)
Where D= Weighted average Consumption for last 5 years

112.2 **Other than Machinery Spares**. For other than machinery spares may be calculated as per following:-

(2.5 X D + NAC + Dues-out) - (Stock held + Dues-in)
Where D= Weighted average Consumption for last 12 months

113 **Functional Requirement**.

113.1 System should be able to set up different forecasting models in the background and be able to tweak standard values to simulate and analyze the different planning results.

113.2 System should be able to let the planners alter the forecasted figures as per Functional Requirements Specifications their personal judgment and be able to save the results.

113.3 System should be able to provide a pre-defined hierarchal approval process to different authorities and enables them to change the figures as per their personal discretion.

113.4 System should be able to provide a mechanism for adding comments by different approval authorities as and when the forecasted plan is changed.

113.5 System should be able to automatically use the available stock, repairable stock or any other category of stock that could be taken as an asset and adjust it against the forecasted figures.

113.6 System should be able to maintain the master data related to reorder point and system to provide alerts as and when the stocks of any of the stock holding nodes fall below an already specified value.

113.7 System should be able to automatically create an order reservation over the next higher node as soon as the stock falls down a specified value.

113.8 System should be able to allow averaging/adjustment of procurement lead time master data as and when the actual lead time overshoots the value defined in the product master.

113.9 System should be able to associate Spare parts with Equipment to enable accurate provisioning.

113.10 System should be able to block provisioning of obsolescent item.

113.11 System should be able to search for product substitution if the substitute has been maintained properly.

113.12 System should identify the surplus of stores.

Goods Receipt

114 **Introduction**. "Good Receipt" process should be responsible to receive and inspection of the items from the vendors against the Supply Order.

115 **Functional Requirement**.

115.1 System should be able to post goods receipt in the system with reference to the supply order.

115.2 System should be able to receive the goods against the supply order and Inspection notes and other delivery related documents given by vendor.

115.3 System should be able to hold the receiving goods in the block stock until the clearance from higher authority or for quality verification is received.

115.4 System should be able to take the printout of good receipt document/ certificate (CRV).

115.5 System should be able to post goods received into quality testing stock and generates an inspection lot for testing based on the inspection plan for the material and also provision to store inspection result.

115.6 System should be able to support gate entry & exit monitoring process for the material & vehicle movements linking with Supply Order or others.

115.7 System should be able to facilitate Partial Goods Receipt.

115.8 System should be able to facilitate Goods Receipt of "Free of Cost" Items/ Samples.

115.9 System should be able to automatically assign stock status such as 'Quality Inspection Stock' if the incoming material is subjected to quality inspection.

115.10 System should be able to incorporate receipt, lot numbers, change in lot numbers of component.

115.11 System should be able to generate bin no wise consolidate report to mustering the receipt items.

115.12 System should be able to reject the items if the lot number is different from the lot given in stock transfer and should have also provision for automatic notification to source echelons.

115.13 System should be able to reject the items if the lot quantity is different from the quantity given in stock transfer and should have also provision for automatic notification to source echelons.

115.14 System should be able to generate the discrepancy report if a lot is found to be degraded or damaged.

Goods Issue

116 **Introduction** “Goods Issue” process should be responsible to issue the items to the demanding units against the Demand.

117 **Functional Requirement.**

117.1 System should be able to generate bin no wise list of items to be taken out as per Issue voucher.

117.2 System should be able to link the packing note automatically while processing Goods Issue transaction.

117.3 System should be able to link the Dispatch note while processing Goods Issue transaction.

117.4 System should be able to issue NAC (Not Available Certificate) for stores.

117.5 System should be able to issue items to stores in lieu. E.g. "Store A" can be issued in lieu of "Store B".

117.6 System should be able to show the status of issue-able stock while processing Goods Issue transaction.

117.7 System should be able to show the progress status of issue voucher on real time basis.

117.8 System should be able to show the indent history i.e. Indent receives to till dispatch or receipt at the destination.

117.9 System should be able to set various statuses to the material stock in case of material 3 across the storage location or shed location.

117.10 System should be able to support the following types of issues:-

117.10.1 Issues against material requests.

117.10.2 Issues against transfer orders (material movement between sites).

117.10.3 Issue against payment book debit to vendors.

117.10.4 Issue of material gains loan request.

117.11 System should be able to track status of indent/ demand.

117.12 System should be able to view and track real time stock position.

117.13 System should be able to maintain approval levels and hierarchies.

117.14 System should be able to check unit demands based on the authorization and scales.

117.15 System should be able to maintain maximum and minimum stock levels for items.

117.16 System should be able to prioritize demands as normal, Urgent, Operational etc.

Physical Inventory Process - Stock taking

118 **Functional Requirements.**

118.1 System should be able to support cycle counting, perpetual inventory, periodic inventory & sampling inventory processes for Physical Inventory (PI).

118.2 System should be able to block materials & storage locations for transaction postings that are identified for PI process.

118.3 System should be able to generate PI counting sheet and capturing of physical inventory count.

118.4 System should be able to calculate PI differences automatically based on quantity as well as value.

118.5 System should be able to define hierarchical approval process for posting PI differences.

118.6 System should be able to define reason codes for PI differences.

118.7 System should be able to report physical inventory adjustment details material wise/ location wise with details of volume and value.

118.8 System should be able to report list of materials for which PI process is pending.

118.9 System should be able to report alerts in case PI process is delayed beyond defined tolerance period or inventory level.

118.10 System should be able to adjust stock position lot wise.

Survey Stocks

119 **Introduction**. Items are surveyed back from the units in different conditions from various ships/units to the Store Depots. These items are surveyed in one of the following categories:-

119.1 Unserviceable

119.2 Obsolete

119.3 Items received in improper condition

119.4 Surplus

119.5 De-storing on decommissioning

120 **Functional Requirements.**

120.1 System should be able to receive material without any demand document like purchase order/ indent or any other demand.

120.2 System should be able to group different kind of scraps according to the nature and lot.

120.3 System should be to record weight and type of Scrap like Metal/ plastic/ Electronic/ Cloth etc.

120.4 System should be able to maintain Restriction List (RL), Segregation List, and List of lots under proof based on the details provided at the time of blueprint stage.

120.5 System should be able to maintain track of in hand quantity of scrap, returned materials.

Warehouse Management System (WMS)

121. **Introduction.** For warehouse management, ICG may track quantity and value of all the materials, perform physical inventory, and optimize warehouse resources. Employees should plan, enter, and document warehouse and internal stock movements by managing goods receipts, goods issues, storage, picking and packing, physical stock transfers, and transfer postings.

122. A warehouse management system (WMS) is a software application that supports the day-to-day operations in a warehouse. WMS programs enable centralized management of tasks such as tracking inventory levels and stock locations. WMS functions typically begin with receipts from suppliers and end with shipments to customers, and include all inventory movements and information flows in between. Warehouse management systems have typically been associated with larger, more complex distribution operations. Small, non-complex distribution facilities have historically not been viewed as candidates to significantly streamline operations and reduce costs.

123. **Functional Requirements.**

123.1 System should be able to maintain store details such as stores, sub stores etc. in the system.

123.2 System should be able to have the storage hierarchy such as location - Bin - Racks -Zones mapped in the system.

123.3 System should be able to view the warehouse storage section layout in document form.

123.4 System should be able to club certain storage bins together for purposes of stocking items such as heavy parts, bulky parts, fast-moving items, slow- moving items.

123.5 System should be able to map the storage details such as volume limitation, type of items that can be stored in a location.

123.6 System should be able to link each and every item image and drawing with its item code for physical identification.

123.7 System should be able to link each item code with its alternate (substitute) item code.

123.8 System should be able to generate the packing list & Dispatch Note against demands from the units.

123.9 System should be able to deduct the stock as soon as the gate pass is prepared in the system for disposed off items.

123.10 System should be able to list down all unapproved Survey Receipt Vouchers (SRV's).

123.11 System should be able to list details of the items not accounted for by stores, along with the reason/discrepancy.

123.12 System should be able to generate alerts to the user; say 3 months in advance for shelf life expiry of an item beforehand.

123.13 System should be able to generate the list of items which have shelf life expiry in a given duration in future says in next 3 months.

123.14 System should be able to issue and monitor inventory items on loan to other departments and thereafter return of the item after usage.

123.15 System should be able to update the bar coded items received/ issued.

123.16 System should be able to maintain different storage conditions according to material storage instructions.

123.17 System should be able to maintain important parameters for sheds like shape, wall thickness, dimensions, distance from other shed etc in document forms loaded in the system.

123.18 System should be able to show location of lots for easy retrieval of the items.

123.19 System should be able for Quality Management Inspection Process to include the qty to be inspected, method of inspection, action in case of discrepancy/ change, action thereof.

123.20 System should be able to allow the process to create kits from individual items and then transfer them to stock.

123.21 System should be able to enable the packing of the items into handling units/ economic issue quantity; also combine multiple handling units into another handling unit.

123.22 Accounting of routine kits in separate ledger folios for ease of accounting and identification.

Equipment Maintenance System (EMS)

124 **Introduction**. EMS should be able to manage online complaint registry mechanism, complaint scheduling to the service engineer both through reports, AMC renewal reminders including AMC/Warranty form creation, product information to officers and MIS reports like spares used, service history, employee productivity etc., are available to enhance the service better. Maintenance can be classified into the following groups:-

124.1 **Preventative Maintenance.** Preventive maintenance can be described as maintenance of equipment or systems before fault occurs. Preventative Maintenance can be further divided into two subgroups:-

124.1.1 Planned maintenance.

124.1.2 Condition-based maintenance.

126.1.3. **Non-Preventative Maintenance**. Non-Preventive maintenance can be described as maintenance of equipment or systems when fault occurs.

125 **Functional Requirements**.

125.1 System should be able to manage and track various documents and statutory requirements for equipment in the system.

125.2 System should be able to define the various maintenance tasks for a equipment/ Assembly/ Sub-assembly that need to be carried out over a period of time in order to keep it in good working condition.

125.3 System should be able to define manpower required for carrying out the various maintenance tasks assigned to each equipment.

125.4 System should be able to edit the spares required for maintenance based on the investigation of problem and indent/demand be created based on the final list defined by the users.

125.5 System should be able to create and maintain the master list of safety instructions/ isolations/ precautions requirements centrally.

125.6 System should be able to update Ship Fit Definition (SFD) with all relevant details like Model NO, Serial number and location in the ship.

125.7 System should be able to approve/edit and own Ship Fit Details (SFD) for all ships of Indian Coast Guard.

125.8 Ability of ships/ professional directorate to request for change of Ship Fit Details (SFD) due to ABER replacement/ Additions & Alterations.

125.9 System should be able to calculate Life cycle analysis of equipment in terms of cost, usage, spares consumptions, cost of manpower etc.

125.10 System should be able to capture life history of equipment & suggest replacement on basis of analysis carried out HQ/ Professional Directorate and availability of workflow for approval and procurement of the same.

125.11 System should be able to identify, amalgamate equipment, parts etc. and plan maintenance activity in a sequence, considering dependency based on user defined conditions.

125.12 System should be able to checklist describing the sequence of individual maintenance activities which is performed repeatedly be created in order to keep the equipment in the running condition.

125.13 System should be able to schedule the checklist for a particular date so as to create the trigger for due maintenance tasks.

125.14 System should be able to carry out preventive maintenance analysis in the system showing the details such as slippage, preventive maintenance to breakdown ratio.

125.15 System should be able to provide the functionality to redefine a workflow activity to the other user in case original approver of the document is absent.

125.16 System should be able to amend the preventive maintenance schedule for equipment if the maintenance was forced/ as per user requirement to carry out on a date other than the original scheduled date.

125.17 System should be able to change preventive maintenance jobs for equipment by assigning a new due date for the preventive maintenance job and ensuring all subsequent cycles follow the new date.

125.18 System should be able to exclude the non-functional equipment from the preventive maintenance schedules.

125.19 System should be able to track the information related to back log orders, equipment replacement recommendations (ABER procedure to be done online for replacement of equipment).

125.20 System should be able to track performance of individual spare/ major item of an equipment.

125.21 System should be able to generate the reports related to TPM (total productivity management) such as number of breakdowns and failures, overall equipment efficiency etc.

125.22 System should be able to generate the alerts/fault reports by the system based on pre-defined threshold values (Rotations, temperatures, vibration, Kilometer, Time etc.)

125.23 System should be able to display non-usage period of the equipment based on the production schedule so that preventive maintenance can be carried out, if any.

125.24 Systems should be able to update equipment related information such as number of hours run, number of parts manufactured, timings utilized etc.

125.25 System should be able to maintain records/ reports of the running hours of the equipment. Submitted online by the ships.

125.26 System should be able to generate the list of spares consumed by the ship while rectifying the defect.

125.27 System should be able to generate a list of spares actually consumed during the refit and its comparison with the initial list of spares demanded for the refit in order to generate and refine the Standard Forecast List.

125.28 System should be able to generate cost of spares consumed in a refit or in a year.

125.29 System should be able to generate reports on the total store demands.

125.30 Maintenance falling due/ spares required/ consumed for preventive or break down maintenance is considered as the key input to forecast spares (ARD) and to achieve inventory management.

125.31 System should able to generate various returns/ report such as technical return, CGSMA returns etc.

Procurement Management

126 **Introduction**. This involves selection and development of sources of supply, placement of orders, follow-up actions, maintaining smooth relationship with suppliers, timely payments, evaluation and rating of suppliers. Proposed procurement management applications give you the visibility into expenditures, key spend categories, contracts and more - helping you drive better-informed supply decisions. Transform your procurement functions with procurement management applications that drive sourcing excellence, procurement compliance, increased efficiency and a streamlined source-to-pay process.

127 Procurement is playing an increasingly strategic role in Indian Coast Guard. Therefore ICG expect more authority, more responsibility, and way more attentions while procurements. But the major obstacles standing in way are Manual legacy processes and procedural bottlenecks, outdated supplier information, sea of papers, and data dispersed across multiple standalone systems and that ever-frustrating eccentric spending from different units for same e=item even when material is available. To manage procurement processes effectively, ICG needs to have full visibility into expenditures, the ability to quickly source key spend categories, insight into total landed costs, and compliance with contracts and policies - so as to realize meaningful efficient and effective procurement. Procurement management functionality should help in automating, simplifying, and accelerating source-to-pay processes for goods and services.

128 **Benefits by adopting e-Procurement**.

128.1 Improved efficiency.

128.2 Cartel formation can be arrested, as any bidder interested will be able to participate with anonymity.

128.3 Fair, free and fearless participation of bidders becomes possible.

128.4 Bring in transparency in tendering process.eduction in costs and processing time for tenders.

128.5 Online Forward & Reverse Auctions will bring better prices.

128.6 Improvement in work culture in the departments.

128.7 Database on goods, services, works and contractors gets built up. Economy of scale is achieved by aggregation of requirements.

128.8 Better access to procurement spending information and analytical reports.

128.9 Saving of Resource, Time, Money & Energy.

128.10 Better Efficiency, Performance and Growth Pattern.

128.11 Healthy Buyer-Supplier relationship and environment

129 **Key Issues in procurement**. Key issues relevant to procurement are as follows:-

129.1 Identifying the needs of customers and suppliers.

129.2 Choosing and preparing tools and processes to communicate with suppliers.

129.3 Preparing requests for proposals and requests for quotations.

129.4 Setting policies for evaluating proposals, quotes and suppliers.

130 Procurement is intended to meet various requirements, essentially, the replenishment of stocks for the ensuing year, and to meet stock out situations. The budget for this expenditure is categorized under the budget for Local Provisioning (LP), and the budget for Central Provisioning (CP). The Local Provisioning Budget is distributed among the Coast Guard Regions and the Store Depots. Coast Guard Headquarters controls the Central Provisioning Budget. RHQ/DHQ makes local procurement based on requirement, and delegated financial powers. Similarly, Director of Logisitcs at Coast Guard Headquarters makes central procurements. The following are the approved methods of procurement in Indian Coast Guard:-

130.1 PAC (Proprietary Article Certificate) Procurement

130.2 Single Tendering Enquiry

130.3 Limited Tendering Enquiry

130.4 Open Tender

130.5 Cash and Carry/ Contingency

130.6 Procurement of spares under refit.

130.7 Repairs under DFPR/ against AWR

131 **Key Functional Requirements - Procurement Solution**. Proposed Solution should enable ICG to:-

131.1 Simplify/ reengineer/ revamp the process.

131.2 Identify savings opportunities through accurate, aggregated spend reporting and analysis.

131.3 Deliver sustainable savings through efficient sourcing capabilities.

131.4 Support automated contract creation, management, and reporting.

132 **eProcurement Life Cycle**. A complete cycle from publishing Tender Notice online to issuing digital Purchase Order including the below processes should be carried out on our portal:-

132.1 Tender Preparation

132.2 Tender Publication

132.3 Tender Promotion through email alerts.

132.4 Corrigendum Publication (if any).

132.5 Vendor Pre-qualification.

132.6 Vendor Registration.

132.7 Vendor Empanelment.

132.8 Tender Document Sale (online and offline payment options).

132.9 Pre Bid Meeting.

132.10 EMD Submission (online and offline payment option.

132.11 Techno Commercial Bid Submission.

132.12 Price Bid Submission.

132.13 Technical and Financial Evaluation.

132.14 Negotiation & Award of Tender.

132.15 Data encryption with PKI support certified by recognized CCA. 128 or higher bit encryption with SSL security.

132.16 Provision of audit trail with log files.

Purchase Requisition

133 **Introduction.** Purchases for goods and services are requested on an approved purchase requisition. Purchase requisitions should be created and approved before a commitment is made to a vendor. The requisition formally authorizes Purchaser to create purchasing transactions (the Purchase order) from budgeted funds. All documentation regarding the purchase (i.e... quotation, proposal, etc.) is forwarded to Purchaser with the requisition for processing and file retention. The purchase order is the primary ordering document for any purchasing activity. It is a formal written offer to a vendor containing all terms and conditions of a proposed transaction. Funds are encumbered against a budget number immediately upon issuance. The purchase order number is the one reference point common to the requisitioning department, purchasing, accounts payable, shipping & receiving and the vendor. It is essential for tracking purposes from the processing stage through the payment stage.

134 **Functional Requirements.**

134.1 System should segregate PRs based on the category of request such as Central procurement, local procurement, direct procurement, cash procurement, etc.

134.2 System should optimize the material requirements during MRP calculation for the materials that are common across the locations/sites

134.3 System should modify quantity of Purchase Requisition (PR) based on new material request and be able to change competent financial authority accordingly.

134.4 System should restrict users on budgetary controls on costs during creation of Purchase requisitions and/or during approval of purchase requisition.

134.5 System should suggest/ Alert users in need basis.

134.6 System should prioritize PR's based on material requirements (urgency).

134.7 System should create PRs in the system through an interface in e-procurement system.

134.8 System must also be capable of recording manually PAC accorded by competent authority.

134.9 Professional directorate should able to generate PR (B-Form) for initial provisioning of E&SP.

134.10 System should able to raise purchase requisitions from demands, Reviews, B-Forms and Forecast.

134.11 System should able to distinguish PR based on sources of supply via Indigenous and Import indent.

134.12 System should capable of handling multiple items in same PR.

134.13 A workflow must exist for PR approval, allowing at each stage amendment of quantities.

134.14 System must allow removal of item from PR till such time PR has not been auctioned PR numbering must follow existing LMS convention for PR (Indents).

134.15 Provisioning officer should able to close PR till such time procurement has not been initiated on the index.

134.16 PR approval workflow must cater to Latest Financial Powers of CFA as per powers indicated.

134.17 System to prompt the Procurement officers/ CFA about the last rates quoted by the L1 firm against other PRs where the procurement action has concluded/ in progress in the last 12 months. System to show history of LPP items wise with clause of inflations.

134.18 Ability to club the Purchase Request (PR) and Tender Enquiry (TE) approval by the IFA in addition of recommended vendor by IFA.

134.19 System should update data on PR by CTS prior to approval of the PR System should provide alerts to all concerned officers regarding the status change of the PRs and pending actions.

134.20 System should allow multiple TEs for a single PR Checks for Obsolete/Obsolescent items while creation of PRs.

134.21 Item-Vendor linkage should be available while preparation of PRs. System to create Item-Vendor linkage in case of nonexistence.

RFP & Tendering

135 **Introduction**. A request for proposal (RFP) is a document that an organization posts to elicit bids from potential vendors for a product or service. For example, a new business or a business moving from a paper-based system to a computer-based system might request proposals for all the hardware, software, and user training required to establish and integrate the new system into the organization. One of the key ways in which the public sector buys, or 'procures' goods and services, is via a tender - a formal document which sets out the proposals and requirements of work to be done. The tendering process allows the buyer - in this case, the public sector - to set out their requirements and allows suppliers to submit offers to the tender, showing how they intend to meet those requirements.

136 **Functional Requirements**.

136.1 System to classify the procurement procedure with standard templates depending upon the type of tendering.

136.2 System should create an RFP with reference to the PR and as per user selection and can be award to multiple Vendors.

136.3 System should capture vendor quotation details for materials against the RFQ.

136.4 System should automatically generate cost comparison statements highlighting all of these: Prices (including break up of taxes), Lead times of delivery, Credit Terms, Other terms and conditions.

136.5 System should split RFQ material by following criteria to different PO's:-

136.5.1 Delivery
136.5.2 By material
136.5.3 By manufacturer

136.6 System should create Statement of Case in case of Ships/Unit/Head Quarters for local procurement.

136.7 System should submit Statement of Case for approval in a defined work flow.

136.8 System should attach required documents.

136.9 System should take online concurrence of members using digital authentications.

136.10 System to support the following types of tendering:-

136.10.1 Open
136.10.2 Limited
136.10.3 Single/ PAC (Proprietary Article Certificate)

136.11 System to have a pre-defined evaluation methodology incorporated for vendor selection.

136.12 System should allow single tendering on the grounds of urgency or operational or technical requirements after capturing the reasons for single tender enquiry (STE) and selection of a particular firm is recorded and approved by competent financial authority prior to single tendering.

136.13 System to grant user the flexibility to select the suitable stages for processing the PR through the tendering process (two bid type):-

136.13.1 Techno Evaluation stage
136.13.2 Price bid evaluation stage

136.14 System should create and monitor the two bid tendering process: In case of Indian Coast Guard the Technical evaluation is normally carried out by a Technical Evaluation Committee (TEC). TEC report, once finalized is sent to Competent Financial Authority (CFA) for acceptance.

136.15 System to capture Names and details of TEC members.

136.16 System to forward the TEC board members name for approval to a predefined work flow through Digital File Management System.

136.17 System to capture the commercial evaluation details as per criteria and provide analysis on factors such as:-

136.17.1 Duties and Taxes

136.17.2 Delivery Period

136.17.3 All Inclusive Cost on Delivery etc.

136.18 System to validate and prompt an alert if the total planned duration of processing the PR exceeds the planned duration as defined in annual provisioning.

136.19 System to provide an analysis on how the vendors have performed in previous tenders for various parameters such as service, quality, price etc.

136.20 System to track the history of previous tenders such as budget, number of tenders issued, number of contracts awarded, work effort, etc.

136.21 System to suggest vendor names based on the database of goods/ work/ services vendors maintained.

136.22 System to create tender document which is to be prepared by using standard templates maintained in the system for different types of tendering.

136.23 In case of limited and single source tendering, system to support selection of vendors based on goods/work/services wise approved vendors maintained in the system.

136.24 System to prevent bids from black listed vendors from being processed.

136.25 System to maintain the EMD amount and performance guarantees, to be defined and managed in the system.

136.26 System to support formation of various committees for opening and evaluation to be done at various stages of tendering (E.g. Tender opening Committee, TEC etc.)

136.27 The tender committee formation is done as per delegation. This will involve sending of notifications to the departments selected by the Contracts department, updating of nominations by the concerned departments, approval of the nomination.

136.28 System alerts to be generated in case the nominations have not been made by the due date.

136.29 System to enable identification of committees by a unique number that will be associated with the respective activities of a particular task.

136.30 System to maintain the entire MOM's, notes, communication, etc. for specific task be maintained and managed by the system in repository.

136.31 System to support validation of the received bids with respect to the tender due dates.

136.32 System to prepare bid opening statement along with the details of the EMD, the bidder and the price quoted.

136.33 System to prepare the comparative statement of the bid.

136.34 System to enable pre-pone or extend bid opening dates along with generation of intimation letters to vendors to be supported by the system.

136.35 System to enable tendering process to be redone in case of e-tendering.

136.36 System to enable formation of committees for evaluation as per the delegation of power be supported and managed in the system.

136.37 System to track waiver of EMD requirements in Vendor Database for each vendor/ class of vendor along with the reasons thereof for waiver.

136.38 System to keep the history of similar previous bids and performance and to be retrieved during the evaluation process.

136.39 System to enable the generation of evaluation from the system based on the updated details by the committee.

136.40 System to support user defined workflows for approval.

136.41 System to support updating of quoted prices against the specific components of the Schedule of Quantity and prices in the system.

136.42 System to support comparison of the quoted prices with estimated costs and quotes made in the previous similar bids.

136.43 System to maintain versions of quoted prices to keep track of price modifications based on negotiations.

136.44 System to enable configuration of defined workflows for approval of evaluation report and award of contract to the successful bidder.

136.45 System to enable capturing of performance guarantees in the system.

136.46 System to generate the alerts prior to a specified period before expiry of the performance guarantee.

136.47 System to maintain template for issue of Letter of Intent.

136.48 System to maintain template for Letter of Acceptance.

136.49 System to enable automatic generation of purchase orders/Letter of Award from with status such as draft, final, approved.

136.50 System to generate a list of EMD's to be released to unsuccessful bidders based on information by the finance team.

136.51 System to enable generation of Notice Inviting Tender (NIT).

136.52 Based on pre-defined templates to invite vendor applications for registration.

136.53 System to define the qualification criteria for vendor short listing.

136.54 System to record and manage receipt of applications.

136.55 System to enable constitution of a committee for evaluation of Vendor applications comprising of representatives from multiple departments.

136.56 System to configure workflows for obtaining approval of committee members.

136.57 System to configure workflow for approval of evaluation report as per users' requirement.

136.58 The System to generate Indent Specific CST format to be forwarded physically along with the tender.

136.59 System should allow updating of Pre Bid discussions on a Tender.

136.60 System should trigger notifications for "Partially unattended Indent lines" and to show dues out along with estimated requirement of the item in future.

136.61 System should allow updating of Item rates and as percentage discounts in part/ full.

136.62 System should have a provision to float a tender on E-Procurement Portal.

136.63 The system to approve Tenders on E-Procurement portal without any manual intervention and send mail alerts to the all officers concerned and the vendors.

136.64 System to allow updating of validity dates of Quote and EMD.

136.65 System should allow vendors to quote using E-Procurement portal.

136.66 System to enter a quote without the corresponding TE.

136.67 System to allow different Vendor Code in Quote as against the Tendered Vendor Code on authorization of a vendor as authorized distributer/ nominated by original vendor to quote.

136.68 System to allow updating of Regret quote for those who could not quoted as against the tendered items.

136.69 System to calculate and display Overall L1 and Item wise L1.

136.70 System not to allow feeding of commercial quotes whose technical bids are rejected.

136.71 System to compare between Indian Vendors and foreign Vendors by taking into account CIF value/ CD exemption.

136.72 System should display LPP (Last Purchase Price) successfully executed in the CST (excluding taxes).

136.73 System should display graphical behaviour of price over time through reports.

136.74 System to update all approvals in the work flow using Digital authentication.

Vendor Evaluation

137 **Introduction.** Unless your organization only uses one vendor for each item they purchase, there will invariably be occasions when a decision has to be made as to which vendor gets your business. There are a number of different scenarios when this will occur, for example when the item is purchased for the first time and when an item is no longer single sourced. When a decision has to be made between vendors, the purchasing department will use some vendor evaluation method to be their tool in the decision. If the item is to be bought for the first time, the purchasing department may have contacted a number of vendors and sent them a Request for Information (RFI). Each vendor would then complete the RFI with the information that was required, normally price and terms. The purchasing department would then use these completed quotations, in conjunction with other information they have collected on the vendors, to make short list for further evaluation or make a final selection. The purchasing department would evaluate the vendors based on a number of criteria they had decided upon which may include objective criteria such as price and warranty and subjective data which would include past experience with the vendor. Based on the weightage given to these criteria the purchasing department would be able to fairly evaluate each vendor.

138 **Functional Requirements**.

138.1 System should define quantitative parameters and weightage for parameters for vendor evaluation like: conformity to delivery schedules, compliance to quality standards, instances of short supplies, pricing.

138.2 System should define qualitative parameters and weightage for parameters for vendor evaluation as will be finalised during blueprinting stage.

138.3 Past performance like delivery schedules, post-delivery response, quality of material, response etc.

138.4 System should generate ratings or evaluation matrix to the vendors as per the historical data.

138.5 System should block/ unblock a vendor for further processing of any transaction. Also, System should capture reasons for blocking/ unblocking of vendor.

138.6 System to evaluate vendor performance ratings on user defined parameters with relational weightage defined for each of the parameters.

Contract Management

139 **Introduction.** Contract management is the management of contracts made with vendors. Contract management includes negotiating the terms and conditions in contracts and ensuring compliance with the terms and conditions, as well as documenting and agreeing on any changes or amendments that may arise during its implementation or execution. It can be summarized as the process of systematically and efficiently managing contract creation, execution, and analysis for the purpose of maximizing financial and operational performance and minimizing risk. A major problem in E&SP inventory appears to be the absence of a systematic way of indicating part number changes by the OEM suppliers to the inventory holders. There is a clear need for contractually binding the suppliers to continually and regularly provide information on part number changes to the users to enable smooth performance of inventory management functions.

140 **Functional Requirements.**

140.1 System to maintain procurement/contract related manuals, guidelines, policies, delegation of powers, etc., for centralized access to all.

140.2 System should configure the workflow for review and approval of the type of Contracts to be followed and attach a digital authentication of the approver.

140.3 System should capture information on whether the vendor has signed the various agreements and attaching the signed agreements.

140.4 System should warn/ prevent the user while releasing the contract in case the vendor has not signed the various agreements.

140.5 System should capture the following details in the contract:-

140.5.1 Contract validity dates

140.5.2 Location of Delivery

140.5.3 Material code with description and quantity

140.5.4 Agreed upon rates including breakup of taxes, payment terms, other terms and conditions.

140.6 System should track the history of previous contracts such as Type of Contract (Rate/ Qty/ Value), number of Contracts issued, Validity Period etc.

140.7 System should maintain versions and reason codes for tracking modification.

140.8 System should maintain the standard templates for the creation of contracts or Letter of Award and Letter of Intent, etc.

140.9 System should number a Contract document automatically.

140.10 System should populate the Contract details from the information maintained in purchase requisition, vendor master.

140.11 Ability to support contract amendments during execution based on change requests submitted by the contractors and evaluation of the same by the respective committees.

140.12 System should define and configure the work flow for approval of amendments to the contract terms.

140.13 System should generate the changed contract once the amendments are made.

140.14 System should document each external/ internal correspondence against a contract for issue handling and progress review.

140.15 Ability to maintain the version control for Contracts in case of amendments to the Contracts with reason.

140.16 System should map the payment terms to the deliverables in the contract.

140.17 System should generate the cost estimates of the contract based on the cost details maintained for the individual items and activities as mentioned in the Indent.

140.18 Ability to capture annual contracts with quantity discounts but no predetermined rates.

140.19 System should capture annual contracts with rates/ quantity discount revised periodically.

140.20 System should capture annual contracts with a fixed percentage discount on list price at any point of time during the year.

140.21 System should capture contract expiry dates.

140.22 Ability to generate alert for expiry of contract to approving/contract concluding authorities as early as six months prior to expiry.

140.23 System should renew the contracts using E-Procurement.

140.24 System to provide option to upload DG&D Rate contracts.

Purchase Order (PO)

141 **Introduction**. A sales contract between buyer and seller detailing the exact merchandise or services to be sourced from a vendor. It will specify payment terms, delivery dates, item identification, quantities, shipping terms and all other obligations and conditions.

142 **Functional Requirements**.

142.1 System to enable creation of PO with reference to Contracts/ PRs.

142.2 System should segregate PO based on the category of procurement such as Cash Purchase, Direct Purchase, and Local Purchase.

142.3 System should create POs with different number as per LMS convention Central purchase & Local purchase.

142.4 System to restrict purchase in case the value exceeds the prescribed cash purchase powers of the designated authority.

142.5 System to handle the Cash purchases, Local Purchase to meet immediate requirements of items required in small quantities and up to certain value limits within the prescribed cash purchase powers of the CFA.

142.6 System should segregate the approval process based on the type of PO.

142.7 Purchase order and amendments (System should add to an existing PO-new items, change quantities and pricing info).

142.8 Ability to define/ configure hierarchical approval process for PO approval based on user parameters such as departments/ type of materials/ Value etc.

142.9 System should capture status (i.e. accepted/ rejected) at every stage of PO approval process with reasons for acceptance/ rejections. Also, System should attach supporting documents/ reports at every stage.

142.10 System should capture the following details in the PO: Date and location of Delivery, PR number, Material code with description and quantity, agreed upon rate including breakup of taxes, payment terms, other terms and conditions, VAT, etc.

142.11 System should automatically populate the prices, taxes, tax rates, terms & condition etc.

142.12 System should automatically generate purchasing schedules based on the material requirement calculations carried out by the system.

142.13 Purchase order auto transmission over email as an option.

142.14 Facility for centralized and decentralized purchasing.

142.15 System should create PO's with different number series based on purchase type such as location/ material type/ department etc.

142.16 Ability to print POs as per pre-defined format depending upon the vendor/ PSU/ DGS & D/ Import Order etc.

142.17 System should automatically identify the supplier specific terms and conditions and print them during PO print out.

142.18 Ability to automatically identify import documentation requirements during purchase order processing and alerting the user to ensure compliance of import documentation.

142.19 Tolerance for excess and short supply. Reporting on excess/ deficit deliveries for a PO.

142.20 Ability to create a PO tracking sheet which provides the following information:-

142.20.1 Service level agreement (SLA) adherence.

142.20.2 Total PO Turnaround time (TAT) i.e. the time from raising requisition till receipt of material.

142.20.3 Delivery schedule adherence.

142.20.4 Goods receipt notes raised against a PO with open PO quantity details.

142.20.5 System should capture procurement patterns in a year i.e. collect data on material procured during the year, along with vendor details and price.

142.21 System should capture entire asset procurement cycle: asset scheduler, Quotations, PR's, PO's, Asset receipt, deployment, Transferring etc.

142.22 System should define the material specific tolerances (option clause) in the system.

142.23 System to propose/ create the repeat order/ Option clause/ RC Order based on some pre-defined conditions.

142.24 System should relate all the above purchases with budget allocated and spent by the CFA.

142.25 Order or schedules acknowledged by the vendor.

142.26 Date offered for inspection/ Call letter details in system.

142.27 A system to capture Inspection details.

142.28 Clause of LD may to be applied incase delay is there in delivery with approval of procuring agency.

142.29 Material dispatched by the vendor.

142.30 Material cleared at customs (in case of imports).

142.31 Material received at the site.

142.32 System should allow Post Contract amendments like Part No Changes by superseding existing part numbers/ deletions/ marking obsolete.

142.33 System should allow Short closure of contracts/ orders for part qty/ Indent line with tolerance clause.

142.34 System should allow recording of supplements to the contracts.

142.35 System should prepare two orders on different vendors for the same indented item.

142.36 Provisions should be made available for Repeat orders/Option clause/ RC Orders.

142.37 System to provide Various Inspection modes while preparing the order.

142.38 System to allow submission of Certified Receipt Voucher by the store depot.

142.39 System to track banned Vendors and provide alerts while preparing tenders and purchase orders.

142.40 System to allow deletion/ re-tendering of Ordered Items/tendered items lines.

142.41 System to allow amendments of orders having financial and non-financial implications.

SAFAL ERP: AIR INVENTORY AND MANAGEMENT SYSTEM

Introduction

143 CGASD(Goa) is responsible for the material management of aircraft spares (permanent & consumables) including sensors, GSE, GHE, SE&FC spares and POL for DOR, CTK & ALH MK-I aircraft and CGASD(BSR) for ALH MK-III aircraft - HAMS. Typical material management functions carried out include provisioning, receipt, accounting, warehousing and quality assurance, technical services and repair loop management, supply order management. The entire inventory is stocked at CGASD (Goa) and CGASD(BSR).

144 Following functional changes are envisaged by implementation of SAFAL ERP Air Inventory Module: -

144.1 On line transaction processing

144.2 Readily accessible, seamless data bases

144.3 System enforced data integrity

144.4 System enforced policy compliance

144.5 Computer aided decision making

144.6 Automatic monitoring and exception reporting

144.7 Data based forecasting

144.8 Electronic accounting

144.9 Role based access control

144.10 Generating periodical returns/ reports

Business Process Reengineering

145 Indian Coast Guard intends to move to a more responsive environment that provides seamless integration of the primary functional areas of Provisioning, Inventory & Warehouse Management, etc with a view to optimize inventory and at the same time meet customer's expectations by enhancing efficiency and operational effectiveness. The IT system will enhance asset visibility and facilitate generation of timely and relevant periodic reports vital for quick and informed decision making. CGASD(Goa) intends to implement standard enterprise product systems for its existing business processes. However, to suit their existing processes, a change (customization) in the standard enterprise product would be expected.

146 SI is expected to identify and analyse the processes where fundamental change would be required. The SI shall prepare a “To Be” document which will include process enhancements and business process reengineering (BPR) requirements. Further it is expected that SI shall conduct workshops, give detailed presentations which will include the gap analysis and specific recommendations for adoption of new improved business processes by CGASD(Goa). The impact of such process improvements would mainly be on department/echelons within the technical and administrative purview of CGASD(Goa).

147 BPR Objective, approach and methodology should ensure simplification and standardization of processes in vogue, after simplifying the processes are to be reviewed to eliminate the redundant steps/practices. Consequent to this, reengineering of process to be done as per the standard available practices in the proposed enterprise solution. After finalizing the “To-Be” process map, automation through standard enterprise software will be done. Configuring the To-Be processes in the system will be able to address all the defined requirements.

148 The System Integrator is expected to define the BPR requirements with a view to achieve the following: -

148.1 Reduction in levels of safety stocks of Depots/ Units without adversely affecting availability against Authorised ASE.

148.2 Improving the resource planning between CGHQ, HQ CGCs, CGASD (Goa). CGASD (BSR), Units, CGAISs, CGAOTs and CGTLOs.

148.3 Measures to reduce replenishment lead time of spares at Depots and units.

148.4 Measures to improve the lead time of supply/ repair turn-around time of items.

148.5 Optimization of stocking by increasing transparency and flexibility

148.6 Reduction in product variants and dead inventory, back loading of non-moving inventory

149 An indicative list (but not limited to) of recommended BPR interventions along with the potential benefits is illustrated below:-

149.1 **<u>Master Data Management</u>**.

Key Process Area	**Master Data Management**	
Process	**Item Master**	
Key "Existing Business Procedure" Steps	**Recommended BPR**	**Benefits**

1. Masterdata management of Airplane IPC, Supplemental IPC, Vendor publication LCM & STATE done manually	1. A central instance of master data will be available to all users for performance of inventory management function	1. Access to centrally maintained master data for various internal departments/ units shall enhance efficiency.
2. Change in existing master records done by approvals/ instructions from agencies like CGHQ/ OEMs/CGAIS	2. Changes to the existing set of master data must be done by CGASD directly on system	2. Provision to execute change of master data by CGASD.
	3. Access to updated data to all concerned departments in real time. Notification to all users regarding change automatically sent by the system through alert or emails Changes to existing data done on receipt of notification will be executed and percolated on real time basis.	3. Correct identification possible with availability of IPC details
	4. Inclusion of IPC details to facilitate identification and linking of spares with IPCs/ Manufacturer recommended Publication/ Manuals.	4. Duplication in master data be eliminated and would result in reduction of range.
	5. Provision to link JPEG images of items with Part No. to facilitate identification	

149.2 **Supply Chain Management**.

Key Process Area	**Supply Chain Management**	
Process	**Provisioning**	
Key "Existing Business Procedure"	**Recommended BPR**	**Benefits**
Steps		

1 Provisioning is carried out based on historical data like float availability, failure rate, turnaround time forrepairs, consumption pattern of consumables, component life like shelf life, storage life, operational life, obsolescence etc, changes in equipment profile and other trends to predict future demands	1. ERP based forecasting technique by analysing these parameters, for enhanced accuracy in forecast. 2. A mechanism for initiation of interim provision review is to be put in place with a view to avoid stock outs. 3. Stock out at user units resulting in-spite of above would automatically create demand requisition at CGASD and issue action initiated in case of sufficient availability of stocks. 4. Threshold stock levels are recommended to be measured in the system. Visibility across the system is recommended and Automatic demand requisition is recommended to be created in CGASD as soon as the threshold level for an item is reached at a lower dependent echelon. 5. Auto generation of ARD in a specific format based on consumption pattern of last three years.	1. Forecasting techniques will bring more accuracy. 2. Collation of comprehensive demand and BER data at CGASD(Goa)/ CGASD(BSR) on real time basis.

150 **<u>Functional Requirements Specification</u>**. Functional requirements to be categorized as per below table:-

Sl.	SI Responses	Description
150.1	Standard(S) *	Product meets the requirement
150.2	Work Around(W)	Provided with workaround solution without changing the source code.
150.3	Customization(C)	Functionality will be made available through development/changes to base product as per business requirements
150.4	Third Party	Bolt-on (third party software) Software (T) applications will be used to provide the required functionality.
150.5	Not Available(N)	Does not meet the requirement

CGASD Functional Requirements.

151 **Organizational Structure.**

151.1 Ability of system to map air inventory Organisational Structure to included CGHQ, HQCGCs, RHQs, CGASD(Goa), CGASD(BSR), Units, CGAISs, CGAOTs, CGAEHU and CGTLOs and all aviation units.

151.2 Ability of system to establish hierarchical technical relation with units between CGHQ, HQ CGCs, RHQs, CGASD(Goa), CGASD(BSR), CGAISs, CGAOTs, CGAEHU and CGTLOs and units.

151.3 Ability to activate/deactivate relation with units.

151.4 Ability to capture mapping of task organization and work relation with units.

151.5 Ability of system to create unit wise defined roles, capabilities etc.

151.6 Ability of system to define unit wise authorized vs held details in terms of equipment and Spares.

151.7 Ability to maintain Master Equipment and Material List (PIL).

151.8 Ability of system to maintain regularly updated database of units.

151.9 Ability to have a complete asset visibility i.e. system should be able to show complete stores holding of units and items/LRUs/Engine dispatched/in transit. Subsequently, on receipt at destination, updation by respective unit/CGAOT/CGAEHU/CGTLO.

151.10 Ability of the system for addition of new units so necessitated due to operational/ administrative considerations.

151.11 Ability of concerned officer/SO/Civilian staff to delegate the role to another officer/ SO/ Civilian staff temporally/ permanently while proceeding on leave/TY duty and permanent transfer.

152 **Master Data Management.**

152.1 Ability to support all types of data and user defined data types.

152.2 Ability to support multiple organizational hierarchies.

152.3 Ability to support hierarchical models to store and maintain relation units.

152.4 Ability to allow online Organizational Hierarchy editing and restructuring and redefine existing Hierarchies.

152.5 There should be no limit to the number of levels in the Hierarchy.

152.6 There should be provision to manage Hierarchies and Classifications. (There should be Support objects like images, videos, PDFs, HTMLs, Text Blocks and other binary objects).

152.7 Advances image management capability within the tool Images can be converted to thumbnails, resolution changes and dimension changed online.

152.8 Central Master Data Management.

152.9 Ability to Define workflow based data management process to ensure data quality.

152.10 Ability to provide role based access to provide restricted view of fields/ alteration of restricted view of fields and data depending on permission.

152.11 Ability to define valid values for pick lists.

152.12 Ability to define validations to ensure correctness of data entered.

152.13 Allow check-in check-out feature to ensure data consistency.

152.14 System should allow multiple users to enter different parts of the record based on roles and should be able to edit.

152.15 System should allow selected role based activities to be performed while in the disconnected mode from the Central database.

152.16 System should allow real time replication/synchronization of data between the Central Server and the backup server.

152.17 Able to generate Aircraft AOG daily state and other aviation returns based on AOG and access to respective units for updation of data on daily basis and RHQs as dashboard.

153 **Master Material/ Item**.

153.1 Ability to maintain location specific data for the material master.

153.2 Ability to define/ configure/ removal of hierarchical approval process for material master creation.

153.3 Ability to define material coding logic for classification of each item as per the CGASD defined logic/ at least ASE.

153.4 Ability of the system to enable catalogue numbering system.

153.5 Ability to classify items as per the business requirement.

153.6 Ability to group items as per the business requirement.

153.7 Ability to use conversion factors to switch between the pack of items and the items themselves (Kit Management).

153.8 Ability to attach item specification document along with the master (for selected items).

153.9 Ability to generate material number as per the codification scheme and track material on current as well as superseded numbering scheme.

153.10 Ability to classify materials as per the business requirement such as finished product, components, sub-components etc.

153.11 Ability to capture critical material relevant information such as drawing, material Specification, Key Characteristics and Images of Items.

153.12 Ability to group the materials as per specific material types, especially for materials having different end usage.

153.13 Ability of System to capture PILs as received from the OEMs and maintain Equipment -Component Hierarchy.

153.14 Ability of system to capture and maintain units' spares authorization (ASE) and revise data time to time.

153.15 Ability to maintain the complete material master record with all specifications such as base unit of measure, shelf life horizon/storage life, Procurement/planning related master data storage data like binnable, bulk etc.

153.16 Ability to generate an automatic notification to all concerned departments in case of any final approved change to the existing master data set up or creation of new master data.

153.17 Ability to provide a compulsive vetting mechanism for every change in an existing master data set up.

153.18 Ability of system to allocate inventory based on groups called Section Heads.

153.19 Ability to classify materials into:-

153.19.1 'A', 'B', 'C' categories

153.19.2 'C', R', 'P' Categories (Consumables, Returnable and Permanent)

153.19.3 "Repairable" (Cat D), Non repairable (Cat E) Category

153.20 Ability of system to handle following types of material: -

153.20.1 Aircraft spares (Permanent and Consumable) and sensors

153.20.2 POL

153.20.3 GSE, GHE, tools, test equipment and manuals

153.20.4 SE/ FC items/ Spares

153.21 Ability of system to incorporate following Air Store codification scheme in Inventory master: -

153.21.1 Manufacturer Part Number

153.21.2 Supplier part number

153.21.3 Alternate part number (02 types)

153.21.4 NATO Code

153.21.5 DEFSTAN

153.21.6 IPC Chapter, Figure No, Item Number and Edition with provision of incorporating amendments as and when promulgated.

153.21.7 Main Equipment

153.21.8 Item master must be able to associate following attributes to the Item:-

153.21.9 Item Code

153.21.10 Aircraft type.

153.21.11 Warehouse Number and Location.

153.21.12 Item Description

153.21.13 Supply source/supply agency

153.21.14 Item Denomination.

153.21.15 Depot Safety Stock.

153.21.16 Minimum Stock Level.

153.21.17 Upper Stock Level.

153.21.18 Annual Consumption Level/ 03 years computation/ 05 years consumption.

153.21.19 Shelf Life.

153.21.20 Lead Time.

153.21.21 Failure rate.

153.21.22 Turnaround time

153.21.23 A, B, C, D & E Category.

153.21.24 Size of Item.

153.21.25 Weight.

153.21.26 Storage Environment (AC, dust free, open space or other special case).

153.21.27 Image of Item.

153.21.28 Drawing of Item.

153.21.29 Repairable/Non-repairable.

153.21.30 Repair agency

153.21.31 IPC/STATE/LCM Details/ CMM(Component Maintenance Manual)/ Manufacturer publication

153.21.32 Ledger Reference

153.21.33 Unit price per each contract

153.21.34 IPA-Item per aircraft

153.21.35 Time since new (TSN), Time since overhaul (TOH), Cycles since new (CSN), Cycles since overhaul (CSO)

153.21.36 Contract numbers, Repair order numbers and RRC numbers

153.21.37 Permanent/ Consumable /GSE/GHE/ tool/ Sensor LRU (Line Replaceable Unit)/ Sensor SRU (Shop Replaceable Unit)

153.22 Ability of the system to add/edit specification of any item. Facility to close yet able to view old specification.

153.23 Ability of system to record lot specific specifications.

153.24 System must have capability of linking equipment to aircraft.

153.25 System must have capability of capturing additional accessories which may be present with Item.

153.26 Ability of system to link substitute of an import item developed indigenously.

153.27 Ability of the system to block the superseded numbers from procurement.

153.28 Data of maintenance routines should be available with planner to ensure high availability of spares.

153.29 Ability to clearly define the following status of every material whether it is a parent product or the component: -

153.29.1 Active/ inactive'

153.29.2 Obsolete/ obsolescence

153.30 Ability to impose restrictions on consumption of the items grouped under the 'issue in lieu' category in the form of validity date, restrictions on some specific lots etc. (if required).

153.31 Ability to maintain the master data for two scenarios mention below:-

153.31.1 Where item 'A' is issuable in-lieu of item 'B' but item 'B' may not be issued in-lieu of item 'A'.

153.31.2 Where item 'A' is issuable in lieu of item 'B' and item 'B' is also issuable in lieu of item 'A'.

153.32 Ability to enable stock transfer for following scenarios under supersession:-

153.32.1 Where an item is superseded by another item and the stocks of superseded item cannot be issued against the demand for superseding item.

153.32.2 Where an item is superseded by another item and the stocks of superseded item can be issued against the demand for superseding item.

153.32.3 Where the stock of the superseded item is merged into the stock of superseding item.

153.33 Grouping of inventory must be done storehouse wise.

154 **Vendor Master**.

154.1 Ability to capture following information about vendor: -

154.1.1 Vendor name.

154.1.2 Contact Person Details

154.2 Vendor address with contact number and email

154.2.1 Ability to assign list of materials / services that can be procured from the Vendor

154.2.2 Ability to allow updation of address.

154.3 Ability to give warning prior/once EDS/ TAT has expired.

154.4 Ability to black list a vendor with authority and vice versa.

154.5 Ability to list black listed vendors.

155 **Unit Master**.

155.1 Ability to maintain unit (End customer) depot dependency

155.2 Ability to maintain unit locations

155.3 Ability to maintain unit authorization in the system.

155.4 Ability to maintain unit dependency in the system

155.5 Asset Master

155.6 Ability to maintain assets details owned by ICG.

156 **Supply order/ Contract Master**

156.1 Ability of system to maintain records pertaining to supply order/ contract (including SO raised by unit) along with supply status.

156.2 Ability to track PDS of items.

156.3 Ability to maintain a record of quality issues related to supply of spares by vendor.

156.4 Ability to generate requisite returns i.e items pending for supply etc.

156.5 Ability to group invoice as M/s HAL Division/ Vendors.

157 **Details of FPQ (Fixed Price Quotation)**.

157.1 The software must cater for following features for incorporating the elements of Fixed Price Quotation (FPQ):-

157.1.1 Procurement of Aircraft spares (permanent/ consumable/ GSE/ GHE/ Tools)

157.1.2 Servicing Cost of Aircraft/ Engine

157.1.3 Servicing/ Repair Cost of Rotables

157.1.4 Cost of CAT 'A' spares

157.2 Abilityto allow the user to alter the prices as and when changes occurs

157.3 Abilityto calculate/ decide HRC and BER.

157.4 Abilityof the system to add Invoice amount and Q-423 amount

157.5 Abilityto billing operation against supplied/ received spares at CGASD

157.6 Ability to undertake induction details of rotables loaded for repairs by respective CGASDs/ CGAOTs/ GTLOs/units.

157.7 Ability to undertake task regularisation by CGAOTs/CGTLOs in consultation with vendor for particular task year.

157.8 Ability to update repair order details by the CGAOTs/ CGTLOs raised by them.

157.9 Ability to update records of rear line item by respective CGAOTs/ CGTLOs used by ICG against AOG requirement cannibalisation of items during servicing due to unserviceability at M/s HAL. If CAT ' A' /HAL items installed during servicing at M/s HAL, Tracking of old item for Cat 'A' item.

157.10 Ability to record warranty period of CAT 'A' and Cat 'B' item.

157.11 Ability to record dispatch and received date of CAT 'D' item.

Supply Chain Management

158 Demand Management- Provisioning.

158.1 Ability to classify type of items as per the business requirement such as Aircraft spares Permanent, Aircraft spare consumable, POL, GSE/ GHE, SE/ FC spare (Permanent and consumable) Manuals etc.

158.2 Ability to maintain in the Planning system the following general Information:-

158.2.1 Ability of the system to sort Entitlement/Authorization (ASE) unit wise as well as material group wise

158.2.2 Ability of the system to calculate Cat "E" (as a percentage of total entitlement) for material groups that are likely to be rendered Beyond Economical Repair or Beyond Local Repair

158.2.3 Ability of the system to take percentage of repairable stock as receipt

158.2.4 Holdings of the stock (sorted material number wise or Census number wise).

158.3 Ability to maintain the complete material master record aggregated at a material group level with all specifications such as nomenclature, material status etc.

158.4 Access to a group of items in inventory must be role based with higher echelons automatically having the permissions

158.5 Ability of system to allow raising of demands if stock exists, limiting the demand to quantity required as per authorization.

158.6 Ability to display a planning table specific to each material group/ material number.

158.7 Ability to define custom fields in the planning table accounting for different figures in the demand and supply side like available stock, stock in transit, maintenance requirements, safety stock requirements, reserve requirements etc.

158.8 Ability to populate the fields in the planning table based on data/scales/ authorizations maintained as a part of the tale.

158.9 Ability to alter the quantity of reserves in the background based on the requirement and their end use.

158.10 Ability to consider different levels of safety stock requirement in the planning table for different units based on the listing specified in the background.

158.11 Ability to collate safety stock requirements over different periods for different units and group at a material group level.

158.12 Ability to add, subtract, multiply and divide different fields of the planning table either manually or using some customized algorithm in the back ground.

158.13 Ability to drill up, drill down the planning data over different periodicities.

158.14 Ability to display the deficits, delayed stock materializations in different colour codes.

158.15 Ability to carry out planning in simulation modes using different versions.

158.16 Ability to provide a pre-defined hierarchal approval process to different authorities and enable them to change the figures as per their personal discretion. Approval will include endorsement by digital authentications.

158.17 Ability of the system to talk with other add-on applications like Business Intelligence and fetch reports in desired formats on a periodic basis.

158.18 Ability of system to raise demands as per following priority:-

158.18.1 A - AOG

158.18.2 B - URR

158.18.3 C - SOTC

158.18.4 D - Routine Demand

158.19 Ability of the system to manage Auto replenishment (ARS) on Units wise (customer wise) quarterly/ half yearly allowances.

158.20 Ability of the system to block particular item of ARS to be issued to unit on unit’s request.

158.21 Ability of system to issue ARS items unit wise or item wise to all the units.

158.22 Ability of the system to issue part quantity proportionally to all the units If sufficient quantity of stock not available for a particular ARS item.

158.23 MIS must exist for ARS item.

158.24 If part ARS Qty has been issued in previous quarter, the same must be made good in the next quarter or when stock arrives considering MSL & USL.

158.25 Ability of system to issue non-availability certificate (NAC) against demands for which item not available along with vendor details.

158.26 Ability of the system to permit demanding of item only to unit which has indicated one of the following authorities for demanding:-

Sl.	**Authority Type**	**Description**
158.26.1	ASE	Air Store Establishment
158.26.2	SVY	Survey Replacement
158.26.3	TYL	Temporary Loan
158.26.4	WOS	Warrant of Stores
158.26.5	XASE	in excess of ASE
158.26.6	ABR	ABER Demands
158.26.7	SER	Servicing/ maintenance requirement of aircraft or GSE/ GHE
158.26.8	Replenishment	Replenishment of item

158.27 Ability of system to check approving authority

158.28 Ability of system to check approval of competent authority to raise PTS demand.

158.29 Ability of the system to check the availability of valid survey reference for demands with SVY reference system.

158.30 Ability of system to check that replenishment demands are only raised for consumable items.

158.31 Ability of system to allow planner to close the demand under following circumstances: -

158.31.1 On request of customer

158.31.2 Delivered

158.31.3 Ex portfolio regularization

158.31.4 Fully complied

158.31.5 Invalid Demand

158.31.6 Multiple Demand

158.31.7 NAC issued

158.31.8 Part complied and closed

158.31.9 Major Servicing completed

158.31.10 Obsolescence of item

158.31.11 Expiry of demand validity (permanent 01 year, consumable 06 months)

158.32 Prior to the demand being put up to the planner it must be vetted by his section

158.33 A workflow must therefore exist.

158.34 The vetting remarks must be viewable by the customer who has raised the demands.

158.35 Ability of system to issue full/ part quantity against demands and closing the demand.

158.36 Ability of system to roll back the issue if the item has not been released by the warehouse staff.

158.37 Ability of planning officer to issue all demands with a single click provided stock available.

158.38 Ability of system to earmark demands for provisioning and priority issuing.

158.39 Ability of the system to account for items issued to M/s HAL, Navy, Airforce, Army on Ty loan/ Permanent basis and generate report.

159 **Demand Planning (Forecasting)/ Distribution Planning Provisioning**.

159.1 Ability to switch between the data of different historical periods while carrying out simulation of the planning results.

159.2 Ability to define specific custom fields for which either the data would be fed manually or extracted from a table in the background. Such fields would be required only if such fields are not available in the standard ERP packages.

159.3 Ability of the system to aggregate and disaggregate the data collated at higher level to the lower levels over different periodicities.

159.4 Ability of the system to have the historical data populated over a planning/ forecasting table sorted by different material-location combinations.

159.5 Ability of the system to disaggregate the changes made to the historical data at the higher node to lower dependent nodes.

159.6 Ability to set up different forecasting models in the background and be able to tweak standard values to simulate and analyze the different planning results along with editing rights.

159.7 Ability to have the different forecasting models attached to the planning/ forecasting table and be able to use them alternatively.

159.8 Ability to carry out the forecast over a pre-defined period in the future based on the historical data and the forecasting model set up in the background.

159.9 Ability of the system to let the planners alter the forecasted figures as per Functional Requirements Specifications their personal judgment and be able to save the results.

159.10 Ability of the system to let the forecasted figures be added, subtracted, multiplied or divided with the figures provided in different customer fields and be able to save the results in a new custom defined field along with editing rights to CGASDs.

159.11 Ability to provide/configure algorithms for any other complex calculations unless otherwise provided as standard.

159.12 Ability to use the standard/configured algorithms by either setting them as default in the background or be able to use them interactively.

159.13 Ability to have different set of forecasted figures

159.14 Ability to provide a pre-defined hierarchal approval process to different authorities and enable them to change the figures as per their personal discretion.

159.15 Ability to provide a mechanism for adding comments by different approval authorities as and when the forecasted plan is changed.

159.16 Ability to automatically use the available stock, repairable stock or any other category of stock that could be taken as an asset and adjust it against the forecasted figures.

159.17 Ability of the system to provide different deployment strategies once the stores have been materialized.

159.18 Ability to percolate the materialized stock on a push model to all lower dependent nodes in exactly the same proportion in which the calls had been placed by them to the central node.

159.19 Ability to provide an option of specifying and changing the percentage of stock that would be pushed to lower nodes based on proportional factors

159.20 Ability of the system to provide an option for distribution from the vendor to all the stock holding location directly.

159.21 Ability to maintain the master data related to reorder point planning.

159.22 Ability of the system to provide alerts as and when the stocks of any of the stock holding nodes fall below an already specified value.

159.23 Ability of the system to automatically create an order reservation over the next higher node as soon as the stock falls down a specified value including shelf life.

159.24 Ability of the system to allow averaging/adjustment of procurement lead time master data as and when the actual lead time overshoots the value defined in the product master.

159.25 Ability of the system to provide an option of maintaining a specified quantity of safety stock and account for the same in planning, for some selected range of items which have a huge lead time but are otherwise very critical.

159.26 Ability of the system to have a pre-defined quantity of stock blocked(Safety stock) to be used only for purposes of AOG or other emergency operations

159.27 Ability to provision for items on life cycle concept

159.28 Ability of system to associate Spare parts with Equipment to enable accurate provisioning

159.29 Ability of system to block provisioning of obsolescent/pre mod/old part number (non superseded) of item

159.30 Ability of the system to search for product substitution if the substitute has been maintained properly.

160 **Demand Management - Review Method.**

160.1 System must provide capability to promulgate review calendar.

160.2 Capability of role based user to generate review for selected item as per calendar.

160.3 Based on inventory type and historical data system must advise the type of planned provisioning to be done for a particular inventory type.

160.4 Ability of system to generate final procurement qty after taking into account pre-defined parameters

160.5 Once new review is generated for an item review should be closed and further indenting must not be allowed.

161 **Demand Management - Provisioning of Aircraft spares, consumables and POL**.

161.1 Ability of the system to carry out a review based on manufacturer and each spares produced by that manufacturer.

161.2 System must be able to compute following inputs for provisioning of spares viz Failure rate (Mean Time Between Failure), Turnaround Time (Mean time of Repair), Annual Consumption, scheduled inspections.

161.3 System must also be able to use following formula for calculating provisional procurement qty (PQ):-

161.3.1 **Aircraft Spares**

Float Required (for Permanent Spares) =A*N +A*N*B+0.15*IPA*N

Where N = No of aircraft in the fleet.
IPA= Items per aircraft

PQ (Consumables BOI Category) = (3D+Dues Out)-(Dues in + Stock Held)

PQ (Consumable Indigenous Category) = (2.5D+Dues Out) - (Dues in + Stock Held)

Where D = Last 3 years average annual consumption.

161.3.2 **SE & FC Spares**

(Permanent PQ spares) = Dues out - (Depot stock + Dues in) + 30 %
(Consumable PQ spares) = Dues out - (Depot stock + Dues in) + 50 %

161.4 Provisioning officer must be able to carry out review of his inventory based on section heads that he deals with.

161.5 Provisioning officer must be able to add or subtract from the PQ generated by the system.

161.6 Approval of review must be based on a workflow.

161.7 System must allow change (with necessary approval of CFA by the indenter) in PQ once consolidation of a review has been done at a higher level.

162 **Demand Management-Initial provisioning of Air stores.**

162.1 Ability of the system to allow CGASD to add/ delete list of spares installed on newly inducted aircrafts.

162.2 System must be able to upload range and scaling data of spares generated by CGASD.

162.3 System must be able to record following information of Range and Scaling document generated by CGASD:-

162.3.1 Part description

162.3.2 Part Number

162.3.3 Total float of the spares in the Coast Guard.

162.3.4 Details of spares manufactured by OEM

162.3.5 Alternate Part Number (2 types)

162.3.6 IPC/ Manufacturer Reference/ Vendor Manual details

Inventory Management

163 **Goods & services Receipt**.

163.1 Ability of the system to post good receipt in the system with reference to the supply order/ Contract/ Repair order/ survey voucher/ Transfer voucher.

163.2 Ability of the system to receive the goods & services against the SO and Inspection notes and other delivery related documents given by vendor

163.3 Ability of the system to hold the receiving in the block stock till the clearance from higher authority or for quality verification

163.4 Ability to printout good receipt (Inspection note & CRV) document or approve with digital sign/ certificate Ability to post goods & services received into quality testing stock and generates an inspection lot for testing based on the inspection plan for the material.

163.5 Ability of the system to capture and track inspection results.

163.6 Ability of the system to allow usage of material only after quality inspection clearance.

163.7 Ability to support gate entry & exit monitoring process for the material & vehicle movements linking with PO or others (packing note/ dispatch advice number).

163.8 Ability to link the goods & services receipt document with the gate entry document reference number.

163.9 Ability to create GR with reference to PO document

163.10 Ability to alert relevant users on receipt of goods & services such as material planning, warehouse and CGHQ

163.11 Ability to capture following key details in the GR document:-

163.11.1 Supplier delivery note/dispatch advice number & date to be included

163.11.2 Vehicle details

163.11.3 Material

163.11.4 Quantity as per supplier delivery note

163.11.5 Quantity as per physical count of stores-in-charge

163.11.6 Returnable material (for e.g. supplier pallets, containers, cylinders etc.)

163.11.7 Receipt condition (i.e. rusted, damaged, OK)

163.11.8 Mode of packing (wooden, carton, gunny bundle, cloth bundle etc)

163.11.9 Weight and dimension of the items.

163.12 Ability of facilitate Partial Goods & services Receipt. The status of invoices cleared and pending should be deduced. Details of payments with details should be available.

163.13 Ability to define & control goods & services receipts against purchase order as per the control policies (e.g. under receipt tolerance, over receipt tolerance etc)

163.14 Ability to block GR process in case the received quantity exceeds PO quantity tolerance limits

163.15 Ability to facilitate Goods & services Receipt of "Free of Cost" Items/ Samples

163.16 Ability to receive the processed 'Job work' materials

163.17 Ability to automatically earmark storage location of the received material.

163.18 Ability to automatically assign stock status such as at QA, at MP, at binning stage etc

163.19 Ability to define receipt conditions such as 'Serviceable, Unserviceable, BER/ CAT 'E'/ Scrap obsolete. As is condition etc. and assign the same during the goods & services receipt process.

163.20 Ability to create and monitor gate entry & exit pass process

163.21 Ability to use handheld terminals inside the depots where electricity power is not available with limited functions of verification, conditioning. Details can be entered on the terminals and updated into the system when terminals are returned to the docking station.

163.22 Ability to execute transactions at warehouse through handheld terminals and maintain record thereof

163.23 Ability of Inspection results are entered into the system.

163.24 Ability to restrict dispatch of item without completing technical inspection.

164 **<u>Goods & services Issue</u>**

164.1 Ability of system to create the indent/request automatically based on the below scenario. The Planning data maintenance is automatically done by the system for every existing item / location combination. The calculations forthreshold would be based on average monthly issue patterns noticed in the past, total liability period for every specific item etc. As soon as the threshold level is reached at a particular echelon, this based on the Planning data done by the system.

164.2 Ability of system to accept manual entry of demands

164.3 Ability of system to check the authorization and scales of unit (requisitioned) while processing Goods & services Issue transaction

164.4 Ability to issue NAC (Not Available) for stores.

164.5 Ability of system to show the status of issuable stock while processing Goods & services Issue transaction

164.6 Ability of system to show the progress status of Goods & services issue voucher on real time basis

164.7 Ability of system to show the demands history i.e. demands receives to till good dispatch from the echelons

164.8 Ability of system to link the packing note automatically while processing Goods & services Issue transaction

164.9 Ability to perform the Goods & services Issue scenario of Sub contract Transfer (To transfer material from Coast Guard to Other organization)

164.10 Ability to define online approval process for the returnable gate pass creation

164.11 Ability to monitor open gate pass documents i.e. gate pass documents for which materials receipt confirmation from consignee have not been received.

164.11.1 Ability to track status of indent/ demand

164.11.2 Ability to view and track real time stock position

164.12 Ability to maintain and track stock held at unit

164.13 Ability to maintain maximum and minimum stock levels for items

164.14 Ability to prioritize demands as AOG, URR, SOTC, etc.

164.15 Ability to record inspection results.

164.16 Ability to restrict access to reports/ transactions based on authorizations

164.17 Ability to cancel gate pass goods & services issue

166.18 Ability to priorities the demand in case of AOG for same item concurrently at two or more units.

164.18 Ability to issue items on FIFO basis for lifed/non lifed items

164.19 Ability to issue items based on remaining life for lifed item

165 Ability to issue items under warranty at first instance to exploit these stores prior expiry of warranty.

166 **Physical Inventory Process - Stocktaking**.

166.1 Ability to support cycle counting, perpetual inventory, periodic inventory processes for Physical Inventory (PI)

166.2 Ability to block materials & storage locations for transaction postings that are identified for PI process

166.3 Ability to generate PI counting sheet and capturing of physical inventory Count.

166.4 Ability to calculate PI differences automatically based on quantity as well as value.

166.5 Ability to define hierarchical approval process for posting PI differences.

166.6 Ability to define reason codes for PI differences.

166.7 Ability to report reason code wise PI differences posted.

166.8 Ability to report physical inventory adjustment details material wise /location wise with details of volume and value.

166.9 Ability to report list of materials for which PI process is pending

166.10 Ability to report alerts in case PI process is delayed beyond defined tolerance period or inventory level.

166.11 Ability to adjust stock position lot wise.

167 Returned Stocks.

167.1 Ability to maintain records pertaining to CAT 'E'/obsolete itesm.

167.2 Ability to maintain track of in hand quantity of CAT 'E' and returned CAT'E" to MO.

167.3 Ability to generate CAT 'E' survey returns.(as per specified format).

167.4 Survey of CAT ‘E’/ Scrap/ obsolete items through MSTC.

168 Warehouse Management.

168.1 Ability to maintain store details such as stores, sub stores, etc in the system.

168.2 Ability to have the storage hierarchy such as location - Bin - Racks - Zones mapped in the system.

168.3 System should be able to view the warehouse storage section layout in document form.

168.4 Ability to map the storage details such as volume limitation, type of items that can be stored in a location.

168.5 Ability of the system to link each item image and drawing with its item code for physical identification.

168.6 Ability of the system to link each item code with its substitute item code, substitute item image and drawing for physical identification.

168.7 Ability of the system to list down the item codes with its superseded item codes.

168.8 Ability of the system to generate the packing list against demands from the units.

168.9 Ability of the system to list details of the items not accounted for by stores, along with the reason/ discrepancy

168.10 Ability to receive items in a different denomination and account them in one authorised denomination

168.11 Ability of the system to generate alerts for preservation due for items.

168.12 Ability of the system to generate the list of the items due for preservation in a given time period.

168.13 Ability to generate alerts say 3 months in advance for shelf life expiry of an item beforehand.

168.14 Ability of the system to generate the list of items which have shelf Life expiry in a given duration in future say in next 3 months.

168.15 Ability of the system to issue and monitor inventory items on loan to other departments and thereafter return of the item after usage.

168.16 Ability to update the bar coded items received/issued.

168.17 Ability of the system to maintain different storage conditions according to material storage instructions.

168.18 Ability of the system to capture storehouse specifications according to material storage instructions.

168.19 Ability of the system to suggest location for storage of items based on various storage criteria maintained in the system

168.20 Ability of the system to show location of lots for easy retrieval of the items

168.21 Quality Management Inspection Process to include the qty to be inspected, method of inspection, action in case of discrepancy/ change, action thereof

168.22 Ability of the system to maintain following record for the warehouse:-

168.22.1 Record of anti-termite treatment

168.22.2 Record of turnover of items

168.22.3 Record of temperature and humidity control

168.22.4 Ability of the system to maintain stack details record for the shed providing information like Sub Depot, Item No. Designation, Store House, Bay No, Stack No, Batch/Lot No, Accounting Unit, Ref Date, Receipts Qty, Issue Qty, Boxes (Full, Partial, Quantity), Rounds Qty, Nature of Packages, Conditions etc.

168.23 Ability of the system to capture firefighting equipment, maintenance plan and location of firefighting equipment fire prone materials.

168.24 Ability of the System to manage All vehicles entry and exit through a checkpoint/ Traffic Branch. The checkpoint/ Traffic Branch are where the registry of the arrival of vehicles and Transportation means in the depot and their departure from it is recorded.

168.25 Ability to continue with warehouse activities while Inventory Audit Count is in process in case of operational requirements/ emergencies

168.26 Ability to actively intimate to dependent units about issue of stores on push model

168.27 Ability to define a Strategy to find a storage bin in a general storage area

168.28 Ability of the system to allow the process to create kits from individual items and then transfer them to stock.

168.29 The system should enable advance planning of inbound receipts/ outbound issues of stores linking demanding units, timelines and storage locations

168.30 The system should have the ability to maintain a list of spares which are to be shipped in original container along with shipping instructions (ex. Avoid stacking etc).

168.31 Ability to generate date about calibration data/ due of certain items.

169 <u>Survey of stores</u>.

169.1 Ability of the system to generate a survey request by users. Ability to sentence the same in same condition or change condition and approve

169.2 Ability of the system to categorize the surveyed items as CAT 'A', CAT 'B', CAT 'D', CAT 'E' or any other type.

169.3 Ability of the system to generate different survey types for serviceable, unserviceable, scrap and short supply.

169.4 Ability of the system to capture the sentencing on the surveyed item as Serviceable (CAT 'A' & CAT 'B'), Repairable (CAT 'D'), Scrap (BER (S) & CAT 'E').

169.5 Ability of system to survey permanent and returnable items to survey yards.

169.6 Ability of system to survey consumable stores when no longer required.

169.7 Ability of system to link surveyed items with unit's electronic ledger.

169.8 Ability of the system to create Work flow between units & CGASD for survey

169.9 Ability of the system to log/record the user from demanding an item without getting the corresponding item surveyed.

169.10 Ability of the system to generate survey vouchers having the item code, survey number, sentencing etc.

169.11 Ability of system to charge off surveyed items from units ledger after issue of receipt voucher and approval of CGASD(GOA).

169.12 Ability of the system to update the stock of the serviceable, repairable, BER as per the category and the agency it is sent to.

169.13 Ability of the system to allow recording of user comments/remarks for each item which is to be surveyed and same should flow along with the survey voucher of the concerned unit.

169.14 Ability of the System to follow existing codification of survey No.

170 <u>Repairable (Cat D)</u>.

170.1 Ability of the system to accept the item as repairable or item to be repaired by repair agencies

170.2 Ability of the system to generate Repair order on the repair agencies.

170.3 Ability of the system to segregate repairable from repair/overhaul/shelf life expiry/modification/upgradation items

170.4 Ability of the system to calculate item wise the failure rate and TAT

170.5 Ability of system to generate the request for sending the equipment out for repair.

170.6 Ability of the system provide the functionality to prepare returnable delivery note for the equipment that needs to be sent out for repairs.

170.7 Ability to have the status of the item be changed when sent out to external agency (i.e. To Be Repaired)

170.8 Ability of system to generate inspection report in the system so as to decide on acceptance/ rejection.

170.9 Ability of the system to update the stock when repaired item is taken back on charge

170.10 Ability of the system to capture the cost of the repair.

170.11 Ability of the system to charge off the ledger (Cat D) when item is dispatched out for repairs.

170.12 Ability of system to update induction date and EDC by CGAOTs/ CGTLOs and CGASDs where CGAOTs/ CGTLOs are not co-located.

170.13 Ability of the system to cancel/ change repair order number.

170.14 Ability of the system to amend Repair order viz change item part number and serial number.

170.15 Load items to repair agency as per repair task, if limit exceeds to be intimated.

170.16 Ability to generate data of last 03 years for repair task preparation.

171 Disposal [Cat E/ BER(s)].

171.1 Ability of the system to capture storage area for unserviceable items.

171.2 Ability of the system to identify source locations form where the unserviceable items are received

171.3 Ability of the system to retrieve the value of received stores

171.4 Ability of the system to enable receipt of stores in an accounting unit that is different from its base unit of accounting

171.5 Ability of the system to enable preparation of lots of the received BER stores based on their type viz permanent and quasi permanent

171.6 Ability of the system to show report on the quantum of Cat E inventory received and disposed off during a given period

171.7 Ability to maintain 'S', repairable, obsolete & Cat 'E' stock level separately.

172 **Preservation.**

172.1 Ability of the system to generate request for preservation

172.2 Ability of the system to enable receipt of stores in an accounting unit that is different from its base unit of accounting.

172.3 Ability to have the status of the item be changed when sent out to external agency (i.e. To Be preserved)

172.4 Ability of the system to provide the functionality to prepare returnable delivery note for the equipment/item that needs to be sent out for preservation.

172.5 Ability of system to generate inspection report so as to decide on acceptance/ rejection.

172.6 Ability of the system to update the stock when preserved item is taken back on charge

172.7 Ability of the system to charge off the ledger (Cat D) when item is dispatched out for preservation.

173 Technical Documents.

173.1 Ability of the system to link the items with the specifications and technical drawings.

173.2 Ability of the system to link the old items with the superseded items along with the technical drawings and the specifications.

174 Reporting requirements.

174.1 Ability of the system to generate report on total repairable inventory held with depot.

174.2 Ability of the system to generate repair agency wise report on items for which preparation of repair order is pending.

174.3 Ability of the system to generate report on items which are not returned post repair after expiry of .delivery period

174.4 Ability of the system to generate report on items inducted with particular vendor for repairs.

174.5 Ability of the system to generate report on vendor wise repair orders issued for quarterly as return.

174.6 Ability of the system to generate report of items falling due for preservation for a particular period and also items preserved in a particular period.

174.7 **<u>Note</u>**:- More report generation requirement will have to be catered for during " Existing process " study phase

175 <u>User Access Management And Governance & Compliance</u>.

175.1 Ability of system to provide segregation of duty rules "out of the box", and address multiple backend systems

175.2 Ability of system to identify risks across multiple applications.

175.3 Governance Ability of system to support Master and Derived role creation and usage. With such roles implemented, ability of system to ensure, access is restricted only to the permitted units/departments of organization.

175.4 Ability of system to provide UI suitable for non-technical business users and IT experts

175.5 Ability of system to provide capabilities for Rules Management

175.6 Ability of system to provide audit controls for mitigation of risks

175.7 Ability of system to generate proactive alerts

175.8 Ability of system to enforce risk prevention

175.9 Ability of system to provide automated remedial options when conflicts are found with integrated workflow

175.10 Ability of system to provide the dynamic drill down capabilities to facilitate proactive analysis and problem resolution.

175.11 Ability of system to enable automation of identification of SOD conflicts at each user level.

175.12 Ability of system to prevent false positives in SOD analysis

175.13 Ability of system to provide risk and SoD analysis at user, role, transaction, and authorization object field value levels.

175.14 The Ability of system to perform “what if” analysis across entire landscape so that there is no “Risk” to our development and quality assurance.

175.15 Ability of system to have the simulation facility before the introduction of a changed role against the current users of that role in order to identify hidden risks at the user level.

175.16 Ability of system to enable creation and management of roles

175.17 Ability of system to enable documenting and managing changes to role definition over time including audit trail of all changes.

175.18 Ability of system to enable the user to select the appropriate roles to be assigned to him from the valid Roles.

175.19 Ability of system to analyze the selected roles in a request against the SoD matrix in real time, to prevent any possibility of risk, fraud or violations.

175.20 Ability of system to support automated workflow designed to address needs of business users

175.21 Ability of system to support multiple workflow paths that are automatically selected based on request/ user attributes, including escalation paths.

175.22 Ability of system to automatically assign the user access in requested system based on approved requests such that no user intervention is necessary.

175.23 Ability of system to have the auditable approval request process

175.24 Ability of system to mitigate the violations, when assigning new access which may cause SoD violations and enable the users or approvers to document what additional controls will be implemented to mitigate violation.

175.25 Ability of system to provide secure and auditable privileged user access

175.26 Ability of system to enable the privileged user access to be automatically monitored.

175.27 Ability of system to not impact system performance while auditing and monitoring of usage of the solution

175.28 Ability of system to provide dashboards that display information geared to the needs of different users viz auditors, IT etc.

175.29 Ability of system to generate and distribute reports detailing SoD conflicts and mark those that have an approved exception.

175.30 Ability of system to download and email reports

175.31 Ability of system to support multi-tier authentication where required

175.32 Ability of system to assign activities to roles, and map roles to users

175.33 Ability of system to include parameters on global and user level security

175.34 Ability of system to provide user and user group authorization administration tool to assign security levels to functions and data, and allow the access by users/ by groups with valid security level only

175.35 Ability of system to restrict users from unauthorized access by allowing only the authorized users with valid profile/password to access only the allowed transaction, as well as be capable of logging off unauthorized users

175.36 Ability of system to provide multi-level access management. The following should be provided:-

175.36.1 User identification

175.36.2 Limitation of user rights to perform operations

175.36.3 Data confidentiality provision

175.36.4 User actions audit and protocols

175.36.5 Application role-based access control should enforce separation of duties. Particular administrative and user functions should be restricted to certain roles.

175.36.6 Session limits must exist for the application. For each session type, there must be limits on the number of sessions per user or process ID and the maximum time length of an idle session.

175.36.7 The solution must not enable users to circumvent the intended user interface to access resources in its supporting infrastructure.

175.37 Ability of system to support the following under user account management.

175.37.1 Unique user IDs

175.37.2 Disabling of inactive user IDs

175.38 Ability of system to display an appropriate warning message upon user logon. The warning message need not include the following four general elements verbatim but must convey the same meaning:-

175.38.1 Use of application constitutes the user's consent to monitoring.

175.38.2 Use of application is limited to official Login use only.

175.38.3 Unauthorized use is subject to prosecution.

175.38.4 Notice that this is a Login system.

175.39 Ability to get Feedback from units.

176 **Document Management**.

176.1 Ability to attach documents with Master/ Transactions e-Document/ scanned document to be attached with master data document or transaction document to be referred later on.

176.2 Ability of workflow based documentation - document, which needs approval (electronics authentications) before uploading to system, same to be moved as per pre-defined workflow.

176.3 Ability of system to feature of Document Classification - Classification of documents based on its business usages.

176.4 Ability of document storage & search - Search document by specifying search criteria. It should provide for secure storage and retrieval of documents and provide document search capabilities based on metadata and content of documents.

176.5 Ability of document Versioning - The application must provide for automated and manual version control with a record of change history and status.

176.6 Ability of file Tracking - Tracking an e document based on its approval, physical status

176.7 Ability of documentation Indexing - Indexing of document in terms of Version number, Chapter Number etc

176.8 Ability of document Flow Tracking - Track flow of document with status

176.9 Ability of system for document Collaboration - The proposed application should have standard capability to ensure collaboration of documents among users for viewing, commenting purpose. The collaboration tool should also support document approval process based on CGASD (Goa) practices and have data security features.

176.10 Ability of document viewing - View Document from various transactions

176.11 Ability to inbuilt capability of document Reporting & Analysis - Reports and Analysis on Document status

176.12 Functionality of attachment of document - Attachment of documents with relevant Material, BOM etc. Integration with external files in other popular formats such as PDF, MS Word, MS Excel with a capability to attach such files to digital manuals

176.13 Ability of the system to capture the IPC's, drawings of spare parts and specifications.

176.14 Ability of system to capture the technical manuals in the system.

177 <u>Quality Management</u>.

177.1 Ability to define quantitative parameters and weightage for parameters for vendor evaluation like: conformity to delivery schedules, compliance to quality standards, instances of short supplies, pricing.

177.2 Ability of the system to maintain Master Quality Inspection characteristics

177.3 Ability of thesystem to record the results of the inspection process.

177.4 Ability of thesystem to record defects.

177.5 Ability of thesystem to maintain Quality Assurance Plans (QAP)

177.6 Ability of the system to have dynamic modification of the inspection scope.

177.7 Ability of the system to generate quality certificates.

177.8 Ability of the system to accept the quality certificates and the results of the OEM supplied certificates.

177.9 Ability of the system to maintain inspection reports and results sent by the vendors

177.10 Ability to maintain the records of the quality issues for the vendors for future reference.

177.11 Ability to maintain defect reports and other reports.

178 **<u>Offline Solutions and Interface</u>.**

178.1 Ability of system to operate in offline mode

178.2 Ability of system to work on limited processes of issue, receipt and stock queries (reports) with limited data of last 15 days of few client PCs in a location when the communication is down

178.3 System should be user friendly and easy to use

178.4 Support relevant tasks without assured communications

178.5 Ability of system to re-synchronize data automatically whenever communication becomes available

178.6 Ability of system to integrate seamlessly into ERP-Systems for all end to end process as per the client requirement

178.7 The Offline Solution should support an Architecture of Local Client with a Selected Business Logic

178.8 The Offline Solution should have Local Data on the offline client to carry out the Transactions

178.9 The Offline Solution should support an Architecture of Data Synchronization, Device Administration

178.10 The Offline Solution should support Selected Business Logic Copyfrom the Master ERP System

178.11 The Offline Solution should support the functionalities of

Authorized versus actual inventory in offline mode also

178.12 The Offline Application should support the following:-

178.12.1 Local data offline Device for selected activities.

178.12.2 Data synchronization

178.12.3 Password changes

178.12.4 Non-repudiation

178.12.5 Security incidents trigger actions etc.

178.12.6 Lock device

179 **<u>Management Information System</u>**. Reports will be decided at the time of actual requirement assessment:-

179.1 Ability of the solution to provide the technology to build a business semantic layer that translates data source technology terms to business terms to enable business users to define information requirements without the need to understand the underlying data source technology.

179.2 Ability of system to extract or refresh information directly from within the MS Office application (Excel, PowerPoint, PDF and Word) without the need to export from another existing report.

179.3 Ability of system to have scheduling capabilities based on events, calendars, time (from to) or specific points in time

179.4 Ability of system to have user, group, object, and folder security

179.5 Ability of system to have repository for reusing common report objects across multiple reports

179.6 Ability of system to have Universal Integration with Applications and Portals

179.7 Ability of system to have dynamic and cascading prompts feature

179.8 Ability of system to support multiple export format support including PDF, MS XL, MS Word, RTF and HTML

179.9 Ability so that users can define/change any number of charts and tables with different permutation of the data via a graphical user interface during the course of analysis.

179.10 Ability of system to enable users to perform pivoting to change the permutation of any graph or table to view information in various perspectives during the course of analysis.

179.11 Ability of system to enable users to perform drill down on any graph or table to view the detail breakdown on any value during the course of analysis

179.12 Ability of system to enable users perform complex filtering by defining set operations (union, intersect, minus) during the course of analysis.

179.13 Ability of system to enable users perform complex filtering by defining sub queries (filtering based on results of another query) during the course of analysis.

179.14 Ability of system to allow users to perform automatic sorting based on numbers, alphabets and dates or manually sort them during the course of analysis.

179.15 Ability of system to enable Users to define totals and subtotals as well as leverage on a library of functions to define additional calculations during the course of analysis.

179.16 Ability of system to enable Users to print the report, export the report to other formats (excel, pdf) or e-mail the report to other members in the community during the course of analysis

179.17 Ability of the solution to enable users to setup a schedule to print, export or email the report automatically.

179.18 Ability of the solution to enable user to enjoy freedom of analysis anywhere with off-line mode for analysts on the go. Users can still continue analyzing or modifying the report layout right from their desktop with no network connection. Data synchronization is seamless so no manual updates are required

179.19 Ability of the solution to enable users to quickly see the data changes in reports after a refresh. Changes in the report (increases, decreases, addition, and deletion of data) are highlighted with different colors which are customizable.

179.20 Ability of the solution to enable users to combine data from Microsoft Excel, CSV and txt files and incorporate data into a single report, which can then be shared with other users through the platform

179.21 The System should provide users with the capability to define information about the report so that other users in the community understands what business questions the report answers, the meaning of the business terms used and the link to other related reports.

179.22 The system should have the capability to key in notes to individual respective reports in the form of threaded messages for the purpose of discussion.

179.23 The system should have the capability to map predefined reports to business processes to build relationship between units people, process and information

179.24 The system should have the capability to quickly search for documents based on metadata as well as contents and the searchable to return results for MS Word documents, MS Excel documents, PDF documents and Web Reports.

179.25 The system input be case insensitive, and support for multi words, phrases and negation.

179.26 The solution must allow the users to define the thresholds for each metric and to define the actions and alerts required when these thresholds are met.

179.27 The solution must provide users the ability to record down actions and findings into a forum initiated based on a particular metric. In the forum, team members can see when findings were recorded and who has taken what action. This reduces guesswork and email overload.

179.28 The solution must provide the capability to the administrator to maintain user login and accounts, to maintain and create public folders, to set policies to access rights and authentication, to control and prioritize server resources.

179.29 The solution must allow end-to-end impact analysis i.e. for any change in source system, developers must be able to know which reports/ ETL/ dashboards/ users are getting impacted with the change and ability of system to provide this feature off-the-shelf and in GUI

179.30 The solution must allow end-to-end data lineage i.e. Sitting at dashboard/ report level, user must be able to know the definition of data along with the source and transformations applied on the same and ability of system to provide this feature off-the-shelf and in GUI

179.31 Should be able to embed reports within the process to perform risk analysis.

179.32 Should support/ provide predictive analytics and data mining add-on components in future as per requirements i.e. System should be scalable

179.33 Should have wizard-based application that enables quickly deliver trusted business intelligence information in any application, in any environment through Web - Service.

179.34 The business intelligence platform must support single sign on and directory services for authorization.

179.35 The business intelligence platform must provide a comprehensive user authorization structure that will allow the administrator to set row level security, object/ column access within the semantic layer, secure folders and reports as well as restricting application features based on user roles.

179.36 The business intelligence platform must allow the administrator to define comprehensive security requirement easily with the ability to organize users into groups and inheriting user rights from groups

179.37 The business intelligence platform must support for multiple platforms to protect our investment when the implementation expands to other areas.

179.38 The business intelligence platform must be able to integrate to existing CG web portal easily

179.39 The business intelligence platform must provide a wizard that will allow administrator to define queries as web services based on the semantic later or metadata so that other external applications are able to leverage on the business intelligence platform. This must be done without any programming effort.

179.40 The tool must have the ability to access a broad range of technologies to cater for both the current environment and any new technologies that may be introduce in the future.

179.41 Tool should have Pre-built Metadata package applications for standard ERP applications

179.42 The solution must have the option to provide ability to transform data on a batch or real-time basis

179.43 The solution must provide the ability to only load the latest changes into a table therefore saving time from doing full table scans. It must provide users with Change Data Capture capabilities

179.44 The solution must provide the capability to perform data profiling, data flow design, data mapping routines and debugging within the same designer and graphical user interface.

179.45 Ability of system to allow for any document or report be previewed before printing

179.46 Ability of system to provide user-friendly interfaces and generate graphical reports and queries

179.47 Ability of system to provide utilities to automate report distribution process, so that user is notified after a report is generated to facilitate easy retrieval

179.48 Ability of system to automate report distribution, so that user is notified after report is generated and the user retrieves report after notification

179.49 Ability of system to provide functionality to users in generating reports on their own without involving technical programming

179.50 The reports should be aggregated at appropriate level or broken down for individual levels

179.51 The reports should be available for time frames like weekly/ daily/ monthly/ yearly.

179.52 The reports should be available in MS Excel, PDF and all modern web browsers.

179.53 The report data must support the feature of being exported to Excel, ASCII files, PDF, or HTML or third party reporting tools.

179.54 The reporting feature should support drill down (across reports/within reports), filter and sorting.

179.55 The report should support the view of seeing numbers/ graphs or both on a single display.

179.56 The reporting feature should allow for user based templates to be created and used for reports.

179.57 The system should provide for calculations, filters and exceptions during reporting.

179.58 The reports should be available to users at any time.

179.59 The reporting feature should support the reports to be scheduled to run in batch/background.

179.60 The tool should notify users when reports have been run.

179.61 The schedule to run the reports should be both event-based or time based.

179.62 Ability of system to support the feature of delivering the reports to the online users through email, portal.

179.63 The report should be broadcasted/ sent on e-mails. These broadcasts/ emails must be after due authorization by the appropriate authority.

179.64 Ability of system to support the feature of alerts to be triggered to Management to take proactive decisions

179.65 Ability of system to provide for metadata objects to be viewed during reporting.

179.66 Ability of system to save the report/ queries for repetitive execution as and when required by the users.

179.67 The reporting feature should make the reports available for analysis of both historical and consolidated data across various systems.

179.68 The reporting tool should have the feature to dynamically summarize data without having to rebuild data.

179.69 Ability of system to make any technical reports available for monitoring the performance of data warehousing system.

179.70 The proposed solution should provide for a role-based dashboard with graphical reporting capabilities with executive summary and detailed drill down reports for business process owners, users, auditors, IT security

179.71 It should be possible to further analyze data in excel spreadsheets for doing trend analysis on exceptions to Segregation of Duties or access to Sensitive Transactions rules.

179.72 It should provide the ability to identify users that have exploited access privileges, identify root causes of conflicts and be capable of interrogating the security log.

179.73 It must provide traffic light reporting to assist in the management of exceptions and reporting must be web-based.

179.74 Ability of system to provide graphics and charting capabilities

179.75 Indicative CGASD(Goa) reporting requirements but not limited to following:-

179.75.1 Stock report displayed item/ location wise, group wise segregated according to batch number/ lot number.

179.75.2 Material status report displayed location wise.

179.75.3 Report for the change log/ transaction history, etc.

179.76 Ability to segregate the stock holding data as 'serviceable', quarantined' and 'safety ' stock.

179.77 Supply MIS

179.77.1 Ability of the system to generate indent status report.

179.77.2 Ability of a system to generate EDS expired order report.

179.77.3 Ability of a system to generate EDS expiry due report.

179.77.4 Ability of a system to generate LPP (Last Purchase Price) Components report.

179.77.5 Ability of a system to generate vendor order details.

179.77.6 Ability of a system to generate item -vendor details.

179.77.7 Ability of a system to generate report based on supply order, item and vendor combination.

179.77.8 Ability of a system to generate report having statistics for month, quarter, half yearly and yearly basis.

179.77.9 Ability of a system to generate reports on monthly order list.

179.77.10 Ability of a system to generate Date wise Gangway In reports.

179.77.11 Ability of a system to generate report of pending orders and pending items against an order with vendors.

179.77.12 Ability of a system to generate reports having vendor details

179.78 Provisioning MIS

179.78.1 Demand status report to be generated through system

179.78.2 Review status report to be generated through system

179.78.3 Ability of a system to generate NAC list of items.

179.78.4 Ability of a system to generate report having details of indented items which are due for provisioning.

179.78.5 Ability of a system to generate stock details of demanded items.

179.78.6 Generation of pending demand report by section head/ department section code.

179.78.7 Ability of a system to generate earmark list.

179.78.8 Ability of a system to generate inventory details by department section code

179.78.9 Free Stock list to be generated by the system

179.78.10 AOG/ URR/ SOTC demand status report to be generated by system

179.78.11 Ability of a system to generate unit and item wise issue detail report for a given period.

179.78.12 Survey detail report to be generated by system.

179.79 Warehouse MIS

179.79.1 Ability of the system to generate report of Gangway Out details.

179.79.2 Ability of the system to generate CWH MIS.

179.79.3 Ability of the system to generate inventory details item wise/ group wise/ segment wise etc.

179.79.4 Ability of the system to generate self life expiry list

179.79.5 Preservation report to be generated in the system.

179.79.6 Delivery status report to be generated through system.

179.79.7 Ability of the system to generate Stock delivery details to units.

179.79.8 Ability of the system to generate the list of items with promulgated life and present status.

179.79.9 Ability of the system to generate Gangway Out details.

179.80 Technical Services MIS

179.80.1 Ability of a system to generate repairable stock list.

179.80.2 Survey Stock list to be generated through system.

179.80.3 Ability of a system to generate repair order.

179.81 MS MIS

179.81.1 Ability of the system to generate demand-issue statistics

179.81.2 Ability of the system to generate list of Gangway in items having no SRV. (R&D)

179.81.3 Ability of a system to generate list of new items introduced.

179.82 Disposal MIS

179.82.1 Ability of the system to generate SurveyList.

179.82.2 Ability of the system to generate Surveystatistics.

179.82.3 Ability of the system to generate list sentencing statistics.

179.82.4 Ability of the system to generate surveyhistorydetails

179.83 SRV MIS

179.83.1 Ability of a system to generate SRV list on the basis of SRV item, unit, unserviceable date and date of approval. and date of receipt.

179.83.2 Ability of a system to generate SRV item code wise

179.83.3 Ability of a system to generate unapproved SRV list.

179.83.4 Ability of the system to generate Item list

179.83.5 Ability of the system to generate item specifications.

179.83.6 Ability of the system to generate alternate part number item lists.

179.83.7 Ability of the system to generate obsolescence item list.

179.83.8 Ability of the system to generate substandard stock list.

179.83.9 Ability of the system to generate shelf life of items.

179.83.10 Ability of the system to generate new item introduction list.

179.83.11 Ability of the system to generate repairable stock for items.

179.83.12 Ability of the system to generate stock situation of items.

179.83.13 Maintain and update records pertaining to the unit cost of all the spares for six types of aircraft including ALH Mk-III, TEHH and MMMA.

179.83.14 Maintain and update records pertaining to the cost of servicing of six types of aircraft including ALH Mk-III, TEHH and MMMA.

179.83.15 Maintain and update records pertaining to the cost of repair of rotable/ engine for six types of aircraft including ALH Mk-III, TEHH and MMMA.

179.83.16 Generate requisite returns pertaining procurement of air stores, servicing of aircraft/ engine and repair of rotables.

179.83.17 Link with the system generated ARD (HAL Division wise) so as to ascertain the CFA prior initiating procurement of air stores.

179.83.18 Calculate warranty of air stores and requisite alert message so as to claim the warranty against contract/ supply order.

180 Workflow Management.

180.1 Ability of the system to have the workflow that allows multi-step approval routing. Non repudiation of workflow is to be ensured using Digital File Management System through electronic authentication.

180.2 Ability of the system to have the workflow that allows for multiple levels of management approval.

180.3 Ability of the system to have the workflow which has a rules engine that allows rules to be created to define approval hierarchies.

180.4 Ability of the system to have the workflow that holds transactions in pending status and not commit them until all approvals are obtained.

180.5 Ability of the system to have the workflow that should be able to send notifications when manual intervention is required in a process.

180.6 Ability of the system to have the workflow that should provide a web based end user interface that can integrate with the portal proposed as part of the solution.

180.7 Ability of the system to have the workflow in which it should be possible to create workflow diagrams that can be shared with business users to verify the workflow.

180.8 Ability of the system to have the workflow in which it should be possible to define the process hierarchies top down or bottom up to support distributed workflow process definition.

180.9 Ability of the system to have a management console which would be available to monitor workflow processes and to control processes that have errors in them.

180.10Ability of system to define business rules without the need for programming, including alerts and triggers

180.11Ability of the system to support creation of secondary workflow by any user, post approval, in the main workflow, during any stage of the parent workflow and keep track of the same along with the parent workflow

181 **Audit.**

181.1 Ability of a system to carry out verification of casting and closing balances.

181.2 Ability of a system to save closing balance on a given date.

181.3 Ability of system to check opening balances with saved closing balances of previous audit cycle.

181.4 Ability of a system to link receipt/issue vouchers with transactions

181.5 Ability of a system to conduct higher audit through query based programs.

181.6 Ability of a system record losses, expenses.

181.7 Ability of a system to carry out ABC analysis.

181.8 Ability of a system to track slow and non- moving items.

181.9 Ability of a system to identify over provisioning.

181.10 Ability of a system to authenticate receipt and issue with relevant supporting documents.

181.11 Ability of a system to view the manual document on screen through an integrated document management system.

181.12 Ability of a system to ensure loan issues is authorized by the competent authority.

181.13 Ability of a system to monitor the loan issues to ensure timely return with notification on loan expiry.

181.14 Ability of a system to track and monitor inter service adjustments

181.15 Ability of a system to computerize following ledgers and provide audit facility for each type of transaction:

181.15.1 Main Store Ledger should contain Permanent, Consumables & GSE/GHE/Tools ledgers separately.

181.15.2 Repairable Store Ledger (Cat D)

181.15.3 Ledger of Salvage and Scrap (Cat E)

181.15.4 Dead/ Obsolete Stock

181.15.5 POL ledger

181.15.6 Manuals/ Publication ledger

181.16 System must provide ways of auditing the following documents and checking that values in the vouchers have been correctly posted in the system.

181.16.1 Supply notes/ CRV

181.16.2 Stock report sheets

181.16.3 Transfer Voucher

181.16.4 Survey Voucher

181.16.5 Issue voucher/ CIV

181.16.6 MC notes

181.17 Stock Verification Sheets

181.18 Demurrage Charges

181.19 Ability of system to generate query for dues-in and dues-out and must link to supply orders

181.20 System must provide query for serviceable, repairable, unserviceable inventory monitoring

181.21 Ability to query non-moving and slow moving and fast moving items.

181.22 Ability of system to charge off items disposed through survey to MSTC.

181.23 System must have ability to carry out stock taking periodically

181.24 Ability of audit officer to query list of costly and attractive items and check stock verification carried out.

181.25 Ability of a system to generate and monitor loss statement.

181.26 Ability of a system to maintain an audit trail

181.27 Ability of the system to query all the issues made in a particular period based on the Category of Stores or Types of Issues or Demand Number wise or Customer code wise or Store House wise or Item wise

181.28 Ability of a system to track items charged off but not released or not delivered

181.29 Ability of a system to track all the receipt of items including loan receipts. It should also be able to generate reports of receipts item wise/ value wise/ source wise

181.30 Ability of a system to track transactions where item released doesn't match items delivered.

181.31 Ability of a system to conduct shelf life audit of items, e.g. Items where shelf life already expired or items where Shelf life is going to expire by a particular date.

181.32 Ability of a system to have records of stores after procurement could not be utilized and became obsolete and surveyed.

181.33 Ability of a system to have records of issues made to other services.

181.34 Ability of a system to have categorization of items/stores into different sections and item codes.

181.35 Ability of a system to have records of stock verification/mustering of items on monthly basis.

181.36 Ability of a system to have records of loss statements preferred to charge off loss due to life expiry.

181.37 Ability of a system to find out the minimum/ maximum stock level of a particular item/ store

181.38 Category of "item/ stores" nomenclature wise, along with part/ pattern number may be provide in the index which may appear as popup screen to have a quick reference to facilitate selective audit in r/ o valuable and attractive stores.

181.39 For generating data in r/o. time expired stores for which shelf life has been prescribed viz O rings, Seals, Packings, Oils and Lubricants, Tyres and Tubes etc.

181.40 System should be able to generate list of inventory items without indicating the balance maintained on computerized ledgers on a particular cut off date for facilitating stock verification by the board.

181.41 Extract generated above should form the basis for the stock taking board for verifying the physical existence and data so collected should be posted back to computerized ledger which should automatically compare the same with the available balance in the ledger for generating a discrepancy report.

181.42 Regularization action to be initiated on above report as per orders

181.43 Items consumed in testing for a given period

181.44 Over provisioning (beyond upper stock level) for a given period.

181.45 List of issues unit/ category/ subject wise for a given period

181.46 List of receipts vendor/unit wise/ category wise/ subject wise for a given period

181.47 Ability of a system to verify Stock Verification i.e all items, particular items, items store house wise for a particular period and discrepancy report

181.48 Closing balance of last audit cycle should be freezed and may be viewed in ensuring audit cycle.

181.49 Ability of a system to show ledger based on period i.e part number, category and type wise.

181.50 Abilityof asystem to show generated delivery note month wise

181.51 Abilityof asystem to show items charged off but not delivered.

181.52 Abilityof asystem to show items delivered in partial quantity.

181.53 Periodical review of MSL should be carried out based on past consumption pattern.

181.54 Ability of a system to show details of inventory rationalization (ASE) as and when carried out by executive authority with justification.

181.55 Ability of a system to bifurcate data -store house wise and date wise

181.56 Ability to generate rotables repair task involving units, depot and CGHQ

181.57 Ability to generate aircraft/aero engine repair task involving units, RHQs, CGHQ.

181.58 Contingent bill/ bill submission/passed details.

SAFAL ERP: FINANCE MANAGEMENT

Key Functional Requirements

182 **Major Subsystems**. The proposed software will have the following major subsystems. Requirements & functionalities shall be as decided at time of Blueprint:-

182.1 Initiation of financial proposal.

182.2 Processing of financial proposal.

182.3 Various stages of Financial Approval {like- Approval On Necessity (AON)/ Sanction}.

182.4 Budget estimation Planning.

182.5 Budget allocation.

182.6 Budget Utilisation and Control.

182.7 Dynamic update of budget allocation as per various stage of financial approval.

182.8 Earmarking Funds and Funds Transfer.

182.9 Year end Closing.

182.10 Project management subsystem.

182.11 Contract Management Subsystem.

182.12 Database management subsystem.

182.13 Data exchange subsystem.

182.14 Project subsystem.

182.15 Legacy System Interface.

182.16 DSS System.

182.17 Budget estimation for the current and forthcoming year.

182.18 Budgetary estimates compilation.

182.19 Allocation of budget /Sub allocation of budget.

182.20 Expenditure reporting and Monitoring.

182.21 Preparation of expenditure returns.

182.22 Monitoring committed liabilities.

182.23 Operational Costing.

182.24 Manpower costing.

182.25 The system should have a seamless integration with the command and control structure and automatically generate the financial hierarchical structure based on the command control structure defined in the system.

182.26 The system will have a user module which will allow the ship or the establishment to carry out its financial related activities optimally.

182.27 The module with administrative authorities/ headquarters would have the basic user module plus additional features to carry out its headquarters role. The Administrative Authorities and the headquarters will also be examining the data provided by the users and incorporating it fully or partly into its subsystem.

182.28 The Headquarters and Administrative Authorities are in fact required to consolidate all data from the subordinate units and incorporate it into the database to be forwarded to the next higher authority after including its own inputs.

Budget Estimates Planning

183 Layouts / Reporting.

183.1 System should allow for creation of attractive and simple layouts for data entry.

183.2 Should allow for consistency and similarity between planning and reporting layouts.

183.3 Should allow for creation of different layouts for different Account Heads.

183.4 Should allow for different layouts for Account heads with different expenditure drivers.

183.5 Should allow for different layouts for different versions of Budget like BE, RE etc can be made.

183.6 Should have some pre-defined layouts for Budget Planning.

183.7 Approved budget values can be transferred from budget planning system to budget control system.

184. **Planning Functions**.

184.1 System should have pre-delivered planning functions like Copying, Revaluate, Distribute, etc. are available or user can write his own logic for calculation of planning values.

184.2 System should have pre-delivered planning functions like Unit Conversion/ Currency Translation are available.

184.3 System should allow for currency translation at Fixed Rate or Current exchange rate or other exchange rate types.

184.4 System should have pre-delivered planning functions like Forecasting with different Forecasting Strategies like Average, Moving Average, Weighted Moving Average, Simple exponential smoothing, Linear exponential smoothing, Seasonal exponential smoothing, Trend seasonal exponential smoothing, Linear regression are available. Applicable option of planning to be done will be decided at blueprint stage.

185. **Status Tracking**.

185.1 System should allow for Status Tracking to have a visual status of the overall budget planning exercise at individual task level.

185.2 System should allow for triggering of ERP mails.

185.3 System should allow for maintenance of texts when the status is changed at individual task level.

185.4 In Status Tracking Facility, multiple status' are available like "New", "In Process", "For Approval", "Completed", "Released".

186. **Notes/ Documents.**

186.1 System should allow for attaching of notes at the elements of the command levels which in turn act as budget centre in the system. The whole workflow including the documents associated with the notes should follow a process route as mandated by the type of transaction being carried out.

186.2 System should allow for attaching Notes/ documents for planning of individual Account heads at budget centres.

186.3 System should allow for editing of the attached notes/documents.

186.4 Should enable Bottom up planning which can be aggregated at higher levels.

186.5 Should enable Top down Planning which can be further distributed to lower levels.

186.6 Should enable planning for different versions of budget like PR, PRE, BE, RE and MA.

Budgeting

187. **Introduction**. Budgeting in a business sense is the planned allocation of available funds to each department within a company. Budgeting allows executives to control overspending in less productive areas and put more company assets into areas which generate significant income or good public relations. Budgeting is usually handled during meetings with accountants, financial experts and representatives from each department affected by the budgeting.

188. **Functional Requirements**.

188.1 System should support mapping of chart of accounts from consolidation to appropriate aggregated levels for budgeting.

188.2 System to define budgets for accounting years and periods used for planning horizons.

188.3 System to maintain multiple budget versions and enables control and validations on latest version number.

188.4 System should render the above reports from departments in foreign currency.

188.5 System should define capital and revenue budgets for financial accounts.

188.6 System should define parent/child budgets to allow roll-ups/downs of departmental budgets into higher-level budgets.

188.7 Ability to develop “bottom-up” budget calculated based on detailed parameters as per business requirement.

188.8 System to upload and download budget from Excel.

188.9 Ability to define budget at various levels which can be the profit-Centre/ cost Centre/ key stage wise (at the lowest level) or any consolidation level of the same.

188.10 System should establish and maintain statistical amounts for a budget.

188.11 System should provide narrative fields to describe budget amounts.

188.12 System should Support for multiple budget, re-forecast and strategic plan versions (including comments).

188.13 System should automatically transfer the Approved budget or forecast data in to the funds managements system for usage.

188.14 Ability to perform what-if scenarios based on different business assumptions.

188.15 System should restrict access to budget to base specified limits authorized personnel only.

188.16 System should maintain a baseline budget.

188.17 System should generate additional budget analytics.

188.18 Budget planning by month and by year depending on the budget cycle.

188.19 "Rolling Forecast" report showing actual costs incurred to date, then budget projected through remainder of reporting period to arrive at period forecast.

188.20 Budget levels should allow - actual, quarterly forecast/projections.

188.21 Forecast/projection/budget revision tracking. Maintain baseline.

188.22 Budget/ forecast, then allow and track revisions to the budget/forecast.

188.23 Maintain online history of budget changes, identifying the user who made the change and what changes were made.

188.24 The system should provide the system should record a narrative reason for change with each record.

188.25 System should establish and enforce spending limitations against a budget and spending authority limits.

188.26 System should restrict access based on user or user-group profile tables at differing points in the budget cycle.

188.27 Ability to importing budget, able to validate and edit the uploaded information prior to posting.

188.28 Budgetary control mechanism should exist at the stage of Indent Creation, Purchase Order creation and Vendor Invoice/Payment processing. Detailed tracking of Indent vis a vis budget should be possible. The nature of control shall be decided at time of blueprint stage.

188.29 System should track and report budget item variance for current month, YTD, inception-to-date, fiscal year.

188.30 Ability to maintain the original funding amounts separate from the change amounts, combining the two at the appropriate levels for control checking.

188.31 Ability to compare funding and spending limitations (both plan and actual) at all levels.

188.32 System should summarize to user defined roll-up levels.

188.33 System should view budget by month, quarter, and year for at least five years.

188.34 System should generate the ICG specific reports

188.35 System should link budget heads to Minor Heads and CGDA code

188.36 System should allow Approval of indents/ PO's should be allowed when budget is available.

188.37 System should provide Exchange Rate data for conversion of currencies

188.38 System to link Indent to Budget Codes/ Minor Heads

188.39 System to amend the Budget Head and Minor Heads of the Indents.

188.40 All approvals of the Indents/ TEs/ Orders should be validated against the available budget.

188.41 System to check avail funds for rising of bills.

188.42 System should be able generate Letter of credit for Foreign procurement.

Budget Allocation

189. **Master Data**.

189.1 Availability of multiple dimensions like fund, fund Centre, functional area, funded programs, grants, commitment item for budgeting purposes. Requirements will be decided at time of blueprint stage.

189.2 Time dependent master data is also available.

189.3 Status management for Master Data is available to control transactions.

189.4 Maintenance of Master Data for Budget Account (e) Maintenance of Master Data for Account Head.

189.5 Maintenance of Master Data for Currency Type.

189.6 Maintenance of Master Data for Currency Conversion.

189.7 Maintenance of Vendor Data

189.8 Maintain Budget User Data

189.9 Maintain Rank/ Roles Code.

189.10 Maintain User Code By Rank/Roles.

189.11 Maintenance of Transaction Type.

189.12 Maintain Schedule of Payments (Period, days, month).

189.13 Maintain CDA Section.

189.14 Maintain BC/ Commands/ Unit Code.

189.15 Maintain Budget Expenditure Categories.

189.16 Maintain Financial Power Group

190. **Authorisations**.

190.1 Authorisation control via Roles for different types of Master Data.

190.2 Authorisation control for Expenditure Head data.

190.3 Authorisation control for Activity wise/Transaction Type like Create, Modify & Display.

191. **Operative Budgeting Processes**.

191.1 System should have periodic budgeting is available.

191.2 System should have user entry level control on period based budgeting is available.

191.3 System should have Budget Release Functionality.

191.4 System should have ability to dynamically or User defined derivation of account head(s)/ organization level(s) for budget control.

191.5 System should have workflow for Budget approvals.

191.6 Should have standard budgeting process of Enter, Supplement, Return, Transfer Posting, Carry Forward is available.

191.7 Master/ Detail of Budget Report are available.

191.8 Maintenance and reporting of all estimates.

192. **Budget Control**.

192.1 Should enable Budget Control at Different levels of organization.

192.2 Should enable exercise and monitoring of Budget Control at different levels of Account heads. It should also allow for realizing for the combination of organisational level & Account heads (major & minor heads).

192.3 Should allow budgetary control on Annual budget for Operating Expenditure & on total budget for capital expenditure .

192.4 Should allow for budgetary control for Receipts and Recoveries. Should also allow linking of Revenue/ Recoveries with expenditure to facilitate revenue based expenditure control.

192.5 Should allow for creation of "Predefined Text" to explicate budgetary control for receipts/ recoveries while executing business transactions.

192.6 Should allow defining Exceptions to exempt certain account heads from budgetary control.

193. **Tolerance Profile**.

193.1 Should allow for Tolerance Limits differently for each of the business transaction as decided at time of blue print.

193.2 Should allow for multiple tolerance limit or validation points for Business transaction.

193.3 Should allow for mail alerts to the person responsible on consuming certain level of budget.

193.4 Systems should able to able to incorporate various work flow involving according of financial approval by concern Competent Financial authorities. The budget allocated to HQ/ units should automatically adjust as per Acceptance of necessity, sanction, unit budgeting and CDA bill processing.

194. **Earmarked Fund**. Requirements will be decided at time of blueprint stage.

194.1 Earmarking of funds for scheme(s) or project(s) like building up of new commands, creation of new infrastructure without knowing the exact application of the fund.

194.2 Transfer of Earmarked Fund from one scheme to another scheme is available Earmarked Fund can go through an approval process. Concerned officials responsible for a scheme can approve the funds reservation.

194.3 Usage of earmarked fund can go through an approval process. Concerned officials responsible for a scheme can approve the usage of earmarked fund.

194.4 Upward or downward revision to earmarked funds can be done.

194.5 In case of downward revision, excess blocked budget will be released to the budget head.

194.6 In case of upward revision, system will control till the free budget else will not allow to create the revised higher earmarked fund.

194.7 Earmarked Funds will be reduced by executing a business transaction like procurement or invoicing or payments.

194.8 Earmarked Fund created for a specific scheme is not available for other scheme/ project for usage with system control.

194.9 Detail report to analyze Earmarked Fund and its usage is available.

194.10 Fields in Earmarked Fund are Date and Time of creation, Financial Year, Budget Centre Code, Recipient (Account Head), Amount, Reason, Approved By, Approval Date and Time.

194.11 Funds can be reserved in foreign currency.

194.12 The document numbering can be system-generated or user-input.

194.13 Audit trail is maintained for creation/ changes to Funds Reservation Document.

194.14 Authorisations can be used for restricting user entry based on Organisation Level or Account Head or a combination of both.

195. **Funds Commitment**.

195.1 Funds can be committed by converting the earmarked funds (w.r.t. purchase orders) for an account head/ utilization level.

195.2 System should control that the Funds Commitment created for a specific scheme should not be available for other scheme/ project for usage.

196. **Funds Transfer**.

196.1 Re-appropriation can be done from one expenditure head to another expenditure head i.e. from one minor head to other.

196.2 Re-appropriation can be done from one organizational level to other i.e from one budget centre to other.

196.3 Re-appropriation functionality can be restricted to the designated authority (MOD) by authorization.

196.4 Audit Trail is maintained.

196.5 Re-appropriation process can follow approval procedure based on organizational hierarchy.

196.6 Re-appropriations can be done in foreign currency.

197. **Supplementary Grants**.

197.1 It is possible to add extra budget to account heads/ budget Centres.

197.2 Supplementary Grants functionality can be restricted to the designated authority (MOD) by authorization.

197.3 Audit trail is maintained.

197.4 Supplementary Grants can follow approval procedure based on organizational hierarchy.

197.5 Supplementary Grants can be done in foreign currency.

198. **Surrenders**.

198.1 It is possible to reduce residual budget from account heads/ budget Centres.

198.2 Surrender functionality can be restricted to the designated authority by authorization.

198.3 Audit trail is maintained.

198.4 Surrenders can follow approval procedure based on organizational hierarchy.

198.5 Surrenders can be done in foreign currency.

199. **Recording Actual and Commitment Data**. Update from Feeder systems into Funds Management.

200. **Closing of Accounts**. Requirements will be decided at time of blueprint stage.

200.1 Should allow for doing closing of accounts as per the requirement of service. Closing operation automatically by identifying the date and time for closing activities.

200.2 Should allow for carry forward of Commitments to next period/ year.

200.3 Should allow for carry forward of Commitments with Corresponding Budget to next period/ year.

200.4 Should allow for reversal of carried forward commitment.

200.5 Should allow for carry forward of residual budget to next year or also closure in the current year as per business requirement.

200.6 Should allow for carry forward of Earmarked Funds to next year or also closure in the current year as per business requirement.

200.7 Should allow for dynamic derivation of budget head or account heads for budgets which have been carried forward.

Project Management

201. **Introduction.** Every time a new project is started, a fresh code head is opened for the project and this code head exists till this project is completed. All expenses for this project are met through this code head. The budgeting and expenditure of funds are dependent upon various landmarks that are achieved and these in turn flow down from the special terms and conditions of the contract. It is imperative that the project management system should seamlessly integrate with terms and conditions of the contract and should also allow defining the following to manage the project:-

201.1 Project classification

201.2 Project status

201.3 Project type

201.4 Organization responsible

201.5 Effective tasks and their respective date for the project

201.6 Key members associated and their responsibilities thereof

201.7 Expense categories

202. **Key Requirements.**

202.1 The project management subsystem should have the ability to assign the project and its tasks to the various levels.

202.2 The system should cater to sub projects associated at the task and sub task levels so as to enable effective management and monitoring of subcontracted parts, as well.

202.3 The user should be able to define and incorporate different agreements and contracts like Purchase order, service agreements and map these for monitoring vis-a-vis estimated outflow of funds or lack thereof. The setting up of such agreements should be flexible enough to cater for negotiation with suppliers.

202.4 The system should provide mapping different projects operational structures such as centralized and decentralized ownership.

202.5 The project status should be workflow driven.

202.6 The project management system should link various types of documents, files, images, noting etc at both the projects, as well as, end task level.

202.7 The project management sub system shall be able to carry out budgeting at the various pre-defined levels of work breakdown structure.

202.8 It should be able to sustain various versions of budget at different levels of same project.

202.9 The sub system should be able to budget by different types of time period's eg. Calendar year, financial year, budget calendar etc. and create a relationship between different calendars.

202.10 System should be able to project cost, revenue, total cost, quantity etc. at summary or detailed level or by resource category.

202.11 System must be able to maintain unlimited versions of budget or record of changes if any.

202.12 The system must report the on-line budget approval process through a workflow mechanism, with a facility to make revision till the final budget is frozen. System should also provide a budget history for tracking changes.

202.13 Users must be able to allocate funds to multiple project and / or/ task within a project depending upon functional roles.

202.14 System shall support various types of budget entries but not limited to following:-

202.14.1 Enter directly via applications.

202.14.2 Copy earlier version from the same project and adjust amounts by specified percent.

202.14.3 Enter budget quantities into a system to calculate the amount.

202.14.4 Create budget in a spreadsheet or project management tools like PrimaVera, or MS Project and upload to the project management module.

202.15 The system should provide for a secure role based portal for online access to different project stakeholders to support resource, delivery and financial management.

202.16 The system should help to report following information among other things:-

202.16.1 Overall Project progress and performance.

202.16.2 Project performance by expenditure categories, project

classification at all times.

202.16.3 Comparison of current year/ periods performance against prior year/ project.

202.16.4 Resource requirement including availability and over committed resources.

202.16.5 Operational efficiency by monitoring time lines, activities that exceed budget etc.

202.16.6 Notification on tasks which needs attention (with flexibility for defining needs for attention).

202.17 The system should provide complete visibility and online project information about the following:-

202.17.1 Budget versus actual data (quantity as well as value).

202.17.2 Period to date, quantity to date, year to date and inception to date information.

202.17.3 Committed as well as actual cost at project, tasks and resource level.

202.17.4 Percentage as well as value based information about the work completed and estimated/ remaining to be completed vis-a-vis the budgeted cost.

202.18 Flag off project lines exceeding the budget for monitoring and control.

202.19 The system should provide equivalent features to enable users to view expenditure information.

202.20 Ability to export data in online queries to desktops, spreadsheets & reporting tools.

202.21 The system should be able to maintain and report accounting records at the transaction level in more than one base currency.

202.22 The system should provide the enterprise wide project information and enable analysis of project information across projects.

202.23 The system should have ability to define control by person, expenditure category, utilization and types of changes etc. i.e. to create any combination of transaction controls and also specific effective data range.

202.24 The system should have the ability to create hot keys for entry of time and expenditure for the most frequently used projects, tasks, expenditure types etc.

202.25 The system should have the option of entering the transaction either in batch mode or interactive mode. Batch transaction shall be automated application whereas initial transaction should move to higher authority for approval. The system needs following features besides routing capabilities:-

202.25.1 Ability to change the approving superior.

202.25.2 Entry of optional routing comments.

202.25.3 Ability to copy transaction to new or existing expenditure.

202.25.4 Ability to view all expenditures entered by various users within the project.

202.26 System shall provide ability to change and manage project on cost plus basis. The schedule for such projects should be deliverable and modifiable.

202.27 The system should have capability to change costs through projects owned by other departments and also cross change projects using borrowed and lent transactions.

202.28 The user should be able to do the following: -

202.28.1 Monitor asset utilization

202.28.2 Track subcontracted invoices

202.28.3 Monitor committed costs

202.28.4 Define expenditure classification expenditure costs, data etc.

202.29 Additionally the system should provide the feasibility to extend the standard functionality, user defined logic to provide for complex costs calculation in terms of foreign currency, fluctuation rates or inflation variations.

202.30 The system should allow user to specify the business rules to be used to determine which account to post a transaction.

202.31 The system should support recording of expenses in multiple currencies.

202.32 The system should support various possibilities of project related purchases for example procurement of goods for specific projects/ tasks as well as common procurements of goods for different projects.

202.33 The system should allow recording of shipment information regarding specific project sites and receiving of material and their specific sites.

202.34 The system should support recording of purchase orders for types of project related material/expenditure categories. This information should flow into the project module for expenditure category wise cost capture.

202.35 The system should support accounting expenditure category.

202.36 The system should support recording of inventory in at least two units of measure.

202.37 The system should support online matching of project specific supplier invoice. This information should be updated in project module with corresponding decrease in the total cost of the purchase order.

Contract Management

203. **Introduction.** The design of tables in the basic Financial System has been so done that in cases where the payment for a contract is staggered and is to be made based on a schedule of delivery or activities completion, scheduling of payments is possible and necessary reminders would be available to agencies handling the contracts.

Capital budgets constitute a major part of budget. It is important that the system is able to capture contractual data (laid out in the special terms and conditions in contract) and translate it into project management module. The idea of project management with respect to Financial Management System is to provide feedbacks to the executive about the progress of the capital project and estimate the fund outflow or absence thereof in the current financial year as well as, rescheduling of payments in the forthcoming time period.

204. **Key Requirements.**

204.1 To achieve this the project management system should have a comprehensive contract management sub module that should be capable of handling the following but not restricted to

204.2 The system should be able to support complex contractual needs by providing contract authoring (including standard conditions of contract and special conditions), administration, execution and flow down of contractual information.

204.3 User defined contract document type such as contract of ship building contracts, weapon/ equipment procurement contracts, machinery equipment contracts, land and infrastructure contracts etc.

204.4 Facilitate conversion of contracts to templates and their maintenance for reuse.

204.5 User defined attributes for contracts.

204.6 The user should be able to breakdown the contract work structure to unlimited hierarchies to ensure data regarding sub-contracts and sub contracts can also be incorporated in the system.

204.7 The contract management module should have a repository of standard articles, special articles, standard terms and conditions and special terms and conditions and should be able to categorize these based on the type of contracts being signed so as to ensure over a period of time a library of conditions is available to ensure effective contract authoring.

204.8 The system should be able to record opinions of different parties to the contract, their objections and therefore the various versions and phases through which contract undergoes before being signed.

204.9 The module should be able to assign different business roles to contractual documents and also the responsibilities of personal towards the contractual obligations.

204.10 The module should be able to carry out contract administration task i.e. maintaining the status of the contract, the changes to it and the approval process of the contract.

204.11 The contract management module should also be able to cater for contract funding, raising flags for contracts for which funds are not available and where the funds are in short supply vis-a-vis the payment schedules and allowing manual override functions at pre-determined levels of users.

204.12 For the capital contracts, the modules should be able to carry out deliverables tracking and integrating the same with the other functional modules.

204.13 The contract management module should be able to carry out role based access security of contracts.

204.14 The system should allow flow down of contractual information to various stakeholders both online and in printed format.

Interfacing

205. Offline Import of Data.

205.1 Should allow budget values to be entered from Excel and upload to ERP.

205.2 Should be able upload budget values from flat file.

205.3 Budget values can be entered in Pre-Defined Templates which can be used to enter data at remote locations/ locations without connectivity and later uploaded to system.

205.4 Authorisation/ Security for uploading of file via authorised IP address/ other checks can be done.

206. Auditing Module for CDA.

206.1 Provision for auditing Contingent Bills raised in SAFAL system to be provided to CDA offices under PCDA (Navy), Mumbai.

206.2 Provision to generate text file for uploading to CGDA website.

206.3 For Units of CG and CDA offices not connected to SAFAL (Directorate of Infrastructure, Directorate of Defense Estate, Embarkation HQ, etc) provision for capturing budget & bill booking data by other connected CG offices as decided at blueprint stage.

VERIFIED

207. **Interfacing with other Applications**. Finance module should be able interface with existing Coast Guard applications. System should able to export data and import from such applications as decided at blueprint stage. Details of applications required to be interfaced are placed at ***Annexure-II*** to this Appendix.

Fund Management

208. **Key Functionalities**.

208.1 System to have a seamless integration with the command and control structure and automatically generate the financial hierarchical structure like the budget centre etc based on the command control structure defined in the system.

208.2 System to define different fund Centres over which the funds are accrued/ channelized.

208.3 System to define different fund commitments within each fund Centre.

208.4 The system to assign/allocate budget to each of the fund Commitments

208.5 System to alert/ stop processing of a purchase order in case of non-avail budget.

208.6 The system to allow reallocation/ adjustment between fund Commitments (if required).

208.7 System should track the pending budget amounts in the system.

208.8 System should define a hierarchal approval process in case of switch of funds/ budget between different fund commitments.

208.9 System should sanction all approvals by using Electronic authentications.

208.10 The system to generate reports of expenses per fund commitment.

208.11 System to generate trend reports such as yield from various investment channels in previous months/ quarters etc.

208.12 Placement of fund requirement from lowest level of budget holding authorities (i.e ships/ units etc) to highest level (i.e CGHQ) with a provision of scrutinise the requirement and revise, if required, at various intervening stages like Station DHQ, RHQs & CGHQ etc. The same is required to meet the projection of fund requirement at various stages of the fiscal i.e RE/ BE/ MA and also during the course of fiscal.

208.13 Provision of fund allocation facility from the top most level (i.e. CGHQ) to lowest level (i.e. units/ ships) of budget holding authorities, with a provision of review and change in allocation in between as and when felt necessary (i.e. by CGHQ, RHQs & DHQs/ Stations).

208.14 Real time bill booking data complication network from lowest level of all fund holders (i.e. to substitute of fortnightly returns). At the same time unit-wise corresponding data like head-wise balance fund availability should also be available to know the progress of fund utilization. The same will also help units/ DHQs/ RHQs/ CGHQs to re-appropriate/ revise balance fund from one user to another depending upon the requirement and progress of utilization of fund to achieve the goal of maximum fund utilization within the targeted dates.

General Ledger

209. **Introduction**. Also commonly referred to as an accounting ledger, a general ledger is a primary accounting record used by a business to keep track of all the financial transactions the company makes. All financial transactions, debits and credits, are recorded, or "posted," in the general ledger, regardless of whether or not they also post to a subsidiary ledger (sub-ledger), such as accounts receivable or cash. These values can provide the information used to generate all of a company's financial statements. When the idea of ledgers was first created, physical ledgers were manually kept, usually in books; with the advancement of technology, most general ledgers are now computerized using accounting software. Requirements and features will be decided at blueprint stage.

210. **Features**.

210.1 System allow addition/ marked for deletion/ modification to chart of accounts as per the requirement.

210.2 Ability to support the functionality of financial module to be fully integrated to the logistics and sales modules thus ensuring that the operational and financial books always reflect the same results.

210.3 System should support park & post of documents.

210.4 System support automatic accounting entries for accounts Payable accounting, fixed asset accounting, accounts receivables accounting.

210.5 System support payroll accounting and its integration with financial accounts/ Indian COAST GUARD funds (the integration of HR).

210.6 System should support budget preparation group wise/ Dept. wise/ channel wise/ region wise/ location wise.

210.7 The system support accounting for security deposit and calculation of interest on security deposit amount should be from the system.

210.8 System to handle reporting under accounting standards.

210.9 System track any new general ledger created and any changes made to the existing general ledgers in the chart of accounts for audit purpose (Only authorized person should be allowed to create general ledger master data).

210.10 System should add new general ledger codes to the existing chart of accounts.

210.11 The system allows maintaining approval hierarchy and competent authority approval before the release of cash payment/ receipt above the specified amount.

210.12 The system to generate report on 'goods received but not invoiced' and on 'invoice received but goods not received' and the goods rejected during a period.

210.13 System assist users in routine vouchers entries by creating predefined sample vouchers for frequent use and system post Documents on predefined dates automatically. (System should also identify all predefined provisional voucher, which have not been posted in the books of accounts like rent, electricity etc).

210.14 System allows specifying level of synchronization required for closing the financial periods by the other modules of the ERP application.

210.15 System ensures that all pending activities are carried out before closure.

210.16 System should post adjustment entries in closed period with proper audit trail and authorization.

210.17 System support posting of expenses identified as 'recurring' on a pre-defined logic and should get posted automatically once the program has been executed on a specified date. Entry generated is reversed on the specified date.

210.18 System should make provisions for expenses from the system based on open items at the time of period closing.

210.19 System should stop double payments and have the check for double invoice.

210.20 System should create provisions for all open GR before making provisions for the period.

210.21 System should generate automatic reversal entries on the first day of next period for provision entries created at the period end.

210.22 Periodic and year end closing of accounts be done as per user defined closing calendar.

210.23 Closing balance of the financial year is carried forward as opening balance to the next financial year automatically.

210.24 System facilitates year end closing process by monitoring the closing entries and closing period separately.

210.25 System to maintain monthly accounting periods in the financial year followed by Indian COAST GUARD.

210.26 System to facilitate blocking of entries in particular general ledgers during the open financial period.

210.27 System to detect any differences between sub-ledgers and control accounts.

210.28 System generates contra entries automatically.

210.29 System maintain audit trail of documents created in the system (system should be able to identify the user who created the document, the user who approved the document, user who edited the document and what all has been edited)

210.30 System support document editing option and if yes then.

210.31 User restricts to specific fields as per Indian COAST GUARD requirements. Also all the change made to a document tracked specifying changes made, changes made by, and date of change and sequence of change.

210.32 System have option of compulsory data entry in selected fields as decided by Indian Coast Guard, and will the system stop the user from further processing if the required data is not entered

210.33 System allows the user to review the document before final Posting.

210.34 Budget, once entered in the system be revised and system maintain revised versions for future reference. System track of all the changes made to the budget like date of change the authorized person who changed it and with reason codes.

210.35 System to block and delete GL accounts not in use.

210.36 System creates an audit trail for the GL account created and amended.

210.37 Sales are mapped to the related purchase.

Account Payable

211. **Introduction**. An accounting entry that represents an entity's obligation to pay off a short-term debt to its creditors. The accounts payable entry is found on a balance sheet under the heading current liabilities.

212. **Functional Requirements**.

212.1 System, check and stop creation of duplicate vendor master accounts. (The system could check for duplicate address, PAN numbers or bank account details to avoid duplicate vendor master creation).

212.2 System to generate ageing analysis for the outstanding invoices.

212.3 System makes payment pending alerts as per schedule pay-out dates automatically.

212.4 System to reflect invoice wise outstanding for a particular vendor and for group of vendors.

212.5 Part payment is made against an invoice and balance payment process on a subsequent date.

212.6 System make payment on account to a vendor and later link it to vendor specific invoice or invoices received.

212.7 Payment approval process be mapped in the system as per the ICG requirements, and approval be given through system.(Payments voucher will be prepared by junior staff, for final payments it will be reviewed by the approving authority for releasing the payment).

212.8 Deductions from invoices be recorded under various accounts like cash discount, rebates, charges etc. with reasons for intimating to the vendor.

212.9 Separate Priced Stores Ledgers to be maintained for every stores item with quantity and total value details. System to calculate inventory cost as per either FIFO basis or moving average as decided at blueprint stage.

212.10 System supports three way checking process for processing of invoices. (Three ways check process specifies that goods are received on the basis of purchase order and invoice is accounted on the basis of goods received in the system) as decided at blueprint stage.

212.11 System blocks invoices and vendors for payment along with reason codes.

212.12 System to record and account discrepancies arising out of physical verification of inventories.

212.13 Various kinds of material issues for work/ material returns from work be valued as per user defined logic.

212.14 Transfer of material from one work to another be traced for adjustments in accounts.

212.15 Normal loss and abnormal losses of material issued to a project be treated according to user defined logic.

212.16 System support claim management with respect to material loss/ short supply either to the account of supplier or transporter.

212.17 System track different kinds of advance payments made to vendors in the vendor sub-ledger.

212.18 Currency transactions record values in both the currencies (foreign currency and the Indian currency).

212.19 Advances be given to vendors on the basis of purchase order.

212.20 The system calculates contingent liability for open bill of exchange and open capital accounts.

212.21 To manage payments, advances and deductions to employee vendors.

212.22 System to support the functionality of account for purchases and categorizing the purchases.

212.23 System to allow entering invoices for adhoc purchases, regular and servicing purchase order (PO).

212.24 The system support associate PO-based invoices with corresponding transactions like Purchase order and/ or goods receipt note (GRN).

212.25 System support debit/ credit note for rate differences

212.26 System support to capture vendor TIN number, NSS and

212.27 PAN numbers mandatory fields and further provides for type of transactions where such mandatory fields are to be filled up

212.28 System support different rates (tax as well as purchase) for different line items for the same PO.

212.29 System support automatic generation of accounting entries for PO-based invoices from PO/ GRN details.

212.30 System to provide reference and match PO-based invoices with the PO/ GRN.

212.31 System should record details of the associated tax and miscellaneous charges.

212.32 System should specify if taxes/ charges are to be calculated for each item in the invoice or the entire invoice.

212.33 System should define payment schedules for invoices together with associated discounts and penalties.

212.34 System should indicate if discounts are based on individual invoice values or gross invoice value.

212.35 System should specify if payments are to be made to third parties in case of PO based invoices.

212.36 System should view vendor addresses and modifying them in case of one-time vendors.

212.37 System should capture additional details like vendor's invoice number and date.

212.38 System should raise item based credit and debit notes.

212.39 System should track over-invoicing, return of goods and increase in prices.

212.40 System should record advances against vendor with reference to:-

212.40.1 General reference

212.40.2 Multiple purchase orders

212.40.3 Multiple Performa invoices

212.41 System should provide for regular and automatic adjustment of invoices/ credit notes with prepayments/ debit notes.

212.42 System to facilitate payment to vendors after adjusting prepayments and debit notes.

212.43 System to provide for a report on transporter payments along with the quantity of goods carried and shortages reported.

212.44 Analytical, summary and standard reports that provide an accurate picture of the accounts payable including invoice, tax, payment amount.

212.45 System to allow calculating payment due as per the terms and conditions.

212.46 System to allow track and trace documents through the use of an extensive document numbering scheme.

212.47 System to allow workflow for:-

212.47.1 Streamlining work processes

212.47.2 Alert for the approval

212.47.3 Alert for pending Item for approval

212.48 System to generate report on year-to-date payments made to the vendor

212.49 System to allow capturing information of shortages and accounting for recovering from the transporters.

212.50 System to support receipt of money from vendors (e.g. recoveries, advances etc.)

212.51 System should transfer vendor balances from one vendor to another.

212.52 System should provide details of discounts offered by vendors.

212.53 System should generate report on discounts availed by the ICG.

212.54 System support vendor ageing (based on invoice date and payment terms)

212.55 System to check double invoicing

212.56 System to provide the list of invoices against a PO.

212.57 System to provide reports on:-

212.57.1 PO generated.

212.57.2 Receipts against PO.

212.57.3 Open PO.

212.57.4 Procurement schedule.

212.57.5 PO vendor reports.

213. **Localization Requirements**.

213.1 System allow to maintain various types of taxes requirements such as VAT, Central sales tax, Service Tax, Withholding tax etc.

213.2 System to allow maintain the period for which specific tax rate is applicable.

213.3 System to allow maintain various tax rates applicable to a specified type of tax.

213.4 System should generate purchase register for different parameters.

213.5 System should balance VAT credit to VAT Payable A/c at the period end automatically as decided at time of blueprint stage.

213.6 System should configure VAT credit and VAT payables as per the applicable statute as decided at time of blueprint stage.

213.7 System to adapt to changes in statutes such as the taxation related changes.

213.8 System to generate report on the various capital expenditure incurred during a period.

213.9 System to calculate and account for the import and export taxes.

213.10 System to keep track of the bank guarantee provided for the fulfillment of the import tax liability and the payments against the bank guarantee.

213.11 System to send the alerts to concerned users, when a breakdown/ malfunctions are reported as decided at blueprint stage.

213.12 System to raise Operational demands

213.13 System to charge off on-board spares based on defect related consumption.

213.14 System to maintain ship specific critical list of Consumable and Permanent spares

213.15 System to automatically generate demands based on re-order level for certain critical spares

213.16 System to Query outstanding demands.

214. **<u>Other Financial/ Fund Management Requirements</u>**.

214.1 The finance module of the SAFAL will be used by all stakeholders for entire budget management (Capital and Revenue). This shall include the following processes for allocations/ withdrawals:-

214.1.1 Making on-line allocations to subordinate units/ lower formations both initial and subsequent (supplementary).

214.1.2 Withdrawal of funds from subordinate units/ lower formations.

214.2 Suitable email notifications should be automatically sent to configured addressees on the CG Unified Domain email. The units receiving these allocations can view them online by logging on to the system. The system shall allow users to communicate on CG Intranet using the email-ids configured on unified Domain.

214.3 The system should allow users to generate corresponding letters for allocation and withdrawal from the system without duplication of effort. This feature should be used for printing hard copies of allocation letter for further dispatch as per extant norms.

215. **<u>Withdrawal of Funds</u>**.

215.1 The system shall allow withdrawal of funds from an immediately lower formation, even when adequate balance may not be held by the lower formation (Funds re- distributed to other units by a Budget Centre). This feature shall be provided to cater for requirements of immediate re-appropriations, based on inputs received from end users, during Phases 1 Roll-Out. In such cases, negative balances may be seen for an organisation against a Code Head, wherein, it is importantly that zero or positive balance be restored on priority, by withdrawing funds from other lower formations/ units to whom the funds have been redistributed.

215.2 Soft copy of allocations on SAFAL shall also have to be centrally provided to PCDA(N) periodically. However, extant mechanism of forwarding hard copies of allocations to CDA offices is to continue till further orders.

215.3 Units not connected on CG Intranet, the allocation letters shall be generated through the system which will be dispatched to all outlying units which are not connected on the CGWAN intranet as per existing procedure.

Revenue Procurement

216. **Functional Requirements.**

216.1 The revenue procurement module SAFAL shall allow users to undertake the complete procurement process, starting from raising of Statement of Case (SOC), generating Request for Proposal (RFP), Recording of Price Bids and generation of Comparative Statement of Tenders (CST), Creation of POs/ Sanction letters, recording of Vendor Invoices/ generation of Contingent Bills as also clearing Payments on bookings by CDAs. Processes for Revenue procurements will also be applicable for Revenue to Capital cases on SAFAL.

216.2 The system shall also provide workflows for online routing of cases for comments, recommendation and approvals. The system shall have built-in checks for Funds Availability based on existing allocations and expenditure. Further, various reports on commitments and expenditure are available through the system.

216.3 Purchase Orders(POs) and Vendor Master Data. All units shall be able to use the system for undertaking revenue procurements. All Purchase Orders (POs) shall be recorded /generated for SAFAL. Further, the system shall be able to support all procurements under GFR 145/146. Vendor base will have to be catered on the system. In case a Vendor is not available on the system, the unit should be able intimate details of the Vendor (Vendor Name, Address, Tax Identification No) to the system administrator SAFAL for inclusion in master data.

216.4 Recording of Invoices. All vendor Invoices/ bills for current and preceding FY need to record on SAFAL and all new Contingent Bills have to be generated through SAFAL, whilst forwarding to CDA offices for payment. The unique Contingent Bill No. generated from the system will be used for automatic clearing the bills though the data received from PCDA(N). Area Accounts Office. Two options shall be available for recording of Vendor Invoices:-

216.4.1 Recording of Vendor Invoice against POs raised on SAFAL for the Current FY.

216.4.2 Recoding of Vendor Invoices Against POs not Raised on SAFAL Contingent Bill for all Vendor Invoices against POs raised in last FY (previous to introduction of SAFAL).

217. **Clearing Payments**. Based on the unique contingent bill numbers (generated through SAFAL), payments shall be automatically cleared on SAFAL, upon processing of bookings data from CDA offices. Payment/bookings, which have not been cleared automatically on SAFAL, the system shall be able to clear manually by respective end users/units on SAFAL, using appropriate transaction. Real time bill to bill basis status of CDAs for the budget holders to be generated by the system, so as to take immediate necessary action by them to react and avoid returning of the bills from the corresponding CDA officers and sort out the observations on priority basis to facilitate bill clearance.

218. **Raising of SoC, RFP, CST** System shall support generation of Statement of Case (SoC), Request for Proposal (RFP) and Comparative Statement of Tender (CST). This will help identify and resolve issues if any being encountered.

219. **Online routing of Cases for Approval**. The system shall be able to support online routing of cases for approval to CFA also to IFA wherever applicable as per delegation of financial power.

220. **Processing of Cases under Powers of Higher CFAs**. Where sanctions/ approvals have been accorded by a higher organization for progressing of the case by a subordinate unit, suitable fund allocations will have to be made on SAFAL to the respective subordinate unit, enabling the unit to raise the Purchase Orders and Contingent bills on SAFAL.

221. **Units not connected on ICG Intranet**. For units not connected on CG Intranet offline Adobe Forms shall be prepared for capture of data for upload in SAFAL.

222. **Use of E-Cash Books**. The SAFAL shall provide functionality of e-cash Books for management of Public Funds. This allows online book keeping by respective units and facility of print outs for record and audits.

223. **Management of ongoing works**. All works under AWP / RAWP (RAWP) shall be created as a Project. Every Contract Agreement is to be recorded in the system as a Purchase Order (PO) and linked to the respective AWP / RAWP Project. Details to be finalized at time of Blueprint

224. **Management of Capital Scheme**. SAFAL shall cater for post contract management for Capital Schemes. Each Capital scheme shall be handled as a project in SAFAL except cases progressed as Revenue to Capital Schemes which will follow the same route as Revenue Procurements.

SAFAL ERP: HUMAN RESOURCE MANAGEMENT

225. **Key Functional Requirements**.

225.1 SAFAL ERP should support various HR related process including Administration, Confidential Report (CR), Training, Promotion, Transfer, Verification, Medical, Records, Release, Manpower & Statistics respectively.

225.2 SAFAL ERP to support management of ICG Officer, Enrolled Personnel and Civilian Personnel right from their training, after recruitment to release from service and to assist formulation of rules and policies for the right growth of ICG Officers, Personnel and service. The ERP should enable ICG to provide the manpower of right type to right place and in right number to the various Coast Guard ships and establishments to ensure the highest degree of operational readiness and efficiency at all times.

225.3 Key functional requirements pertaining to HR modules are as follows:-

225.3.1 System should allot P.No.to CG personnel on joining ICG service.

225.3.2 System should have ability to enter the personal data on induction in service.

225.3.3 System should issue appointment list/ order on various occasions.

225.3.4 Facilitation of receipt of authenticated documents for civilian personnel from respective admin.

225.3.5 Record keeping of all service records for civilian personnel in eservice book as existed in central secretariat.

225.3.6 System should calculate default retirement date on attaining the age of superannuation.

225.3.7 System should issue certificate to officers on their retirement/ release.

226. **Major Subsystems**. The proposed software will have the following major subsystems. Requirements & functionalities shall be as decided at time of Blueprint:-

226.1 Manning Plan and Recruitment

226.2 Training

226.3 Transfer

226.4 Promotion

226.5 Release

226.6 Veteran

226.7 Nomination

226.8 Confidential Reports

226.9 Miscellaneous

Manning Plan and Recruitment.

227. **Manning Plan.**

227.1 Maintain details of approved manning plan and Govt sanction for each ICG unit

227.2 Reports on manning plan, Govt. sanction, borne strength as required

228. **Recruitment.**

228.1 Induct recruited Officers, Enrolled Personnel and Civilian Personnel.

228.2 Integrate with ICG recruitment software system.

229. **Training**. ICG officers/ personnel are all nominated for training at various stages of their career starting from induction to pre-release courses. The ERP should support end-to-end activities related to training covering following:-

229.1 Nominate ICG personnel for various courses as per merit.

229.2 Maintain database of course related information.

230. **Transfer**. Coast Guard ships/ establishments are located in different parts of country with varying facilities of married accommodation, education, medical and other allied amenities. The ERP should assist ICG for providing manpower in these billets so as to achieve a high standard of efficiency and also provide equal opportunities to all officers, personnel to serve in different Coast Guard stations so as to enrich their knowledge and experience. Transfer of ICG Officers, Enrolled Personnel and Civilian Personnel is normally effected on one of the following occasions and ERP should support ICG on the same: -

230.1 To meet the manning plan of ships/ establishments/ air squadrons as promulgated by Coast Guard Headquarters from time to time.

230.2 Affording sufficient opportunity to all officers/ personnel to gain requisite experience and to complete prescribed sea/ squadron time for promotion to higher ranks.

230.3 To effect turnover of enrolled personnel on completion of prescribed tenures in ships/ establishments.

230.4 To provide adequate shore tenure with due consideration to shortages in a particular cadre.

230.5 To make up for shortages in a ship/ establishment due to cases of release, marked run or low medical category.

230.6 Extreme compassionate grounds requiring an enrolled personnel presence at one station for a certain period.

231. **Promotion**. Officers, Enrolled personnel and Civilian Personnel fully qualified for promotion to next higher rank in accordance with Rule 20 of Coast Guard (Seniority & Promotion) Rule 1987, shall be eligible for promotion as per the provisions of Recruitment Rules. During promotion, it should be ensured that suitability of the candidates for promotion is considered in an objective and impartial manner.

232. **Release**. The release/ pensionary benefits of Coast Guard enrolled personnel are governed by CCS Pension Rules, 1972 as amended from time to time, incorporating the benefits as per recommendations of the VIIth Central Pay Commission. The ERP should support for release of ICG officers/ personnel on following:-

232.1 Superannuation

232.2 Retiring Pension (Voluntary Retirement)

232.3 Invalid release

233. **Veteran**. Should provide required support for ICG veteran cell. Also enable the system to import the data from ERP to CG veteran web portal.

234. **Nomination**. Various nominations for different types of benefits are required to be submitted by every individual on entry into the service and subsequently on change in marital status, family members. Various forms have been prescribed for different types of nominations and therefore the nominations are to be made strictly in the prescribed form only. The ERP should support submission of nomination forms and management of nomination database.

235. **Confidential Reports (CR)**. The SAFAL ERP should design & develop ICR (Intelligent Character Recognition) based CR related workflow. Required ICR licenses to be provisioned. CR is applicable to all ICG personnel including officers, enrolled personnel and civilian personnel.

236. **Migration of HR data**. Should migrate existing HR data into SAFAL ERPs.

SAFAL ERP: NON-FUNCTIONAL REQUIREMENT

237. **General Features**.

237.1 The solution architecture should be platform and vendor independent.

237.2 Solution should be implemented of 'Responsive Web Design' and Web 3.0 compliant. All customised UI5/UX should be based on ICG SIMHA 'Unified Portal' web theme and design. Application's design should be user friendly and UI 5 supported.

237.3 The solution should provide for multi-tiered architectures.

237.4 System architecture should allow infrastructure simplicity and standardization.

237.5 The solution software should be certified for different types of hardware.

237.6 The ERP should support and implement disaster recovery.

237.7 An integrated portal to view selected information should be developed on SIMHA platform as part of 'Unified ICG Portal' architecture requirements. he solution should be designed to remove all single points of failure. The solution should provide the ability to recover from failures and should also provide clustering features, thus protecting against many multiple component failures.

237.8 The solution should have the ability to scale up as and when the new business applications and services are added without compromising the performance of the overall solution. The architecture should be proven to be highly scalable and capable of delivering high performance as and when the transaction volumes increase.

237.9 The solution should provide application architectures that are highly granular and loosely coupled. The solution architecture design should promote flexible business process management for future scalability. The solution should be interoperable in nature and design and development should be based on Service Oriented Architecture (SOA).

237.10 Should expose data through web services into Enterprise Service Bus (ESB). Central intranet portal shall aggregate required information from SAFAL ERP through ESB.

237.11 The solution is required to cover critical business function and process modules and provide modularity that should support addition / deactivation of one more module through authorisation control. However, these modules should be seamlessly integrated in the core application system.

237.12 The solution architecture allows minimum package modifications so as to preserve the package upgrade path.

237.13 The solution should support standard interfaces such as adapters, APIs to interface with standard application and legacy applications and support user exits.

237.14 The solution should support real-time data updates.

237.15 The application should have automatic way of migrating the data of existing database in case of data structure change during transfer to new versions.

237.16 The solution should support export and import of data possible from different legacy systems/ other systems/ databases in different file formats and on specified time intervals.

237.17 The ERP application should support SSL and digital certificates.

237.18 The solution should be remote access integration compatible.

237.19 Architecture and cluster processing.

237.20 The solution should have no 'Single-Point-of-Failure' at within site level (ie DC, DR, ROBO).

237.21 The solution should support disaster recovery with fail-over and fail-back on both auto/ manual modes between DC, DR.

237.22 The solution should support remote replication of data from ROBO to Central Site and vice versa to ensure RPO is less than 30 minutes. Also, remote replication should offline support 'Store-Forward' of data upto 60 days.

237.23 The solution should support distributed processing.

237.24 The solution should be deployed in high-availability configuration.

237.25 The solution should be cloud-ready.

237.26 The solution should support load balancing.

237.27 Application should have capability of Whitehall file system.

237.28 System should provide capability to user to work on the files as per Whitehall filing system. UI/ UX of the filing system should be user friendly.

238. **Application Architecture**.

238.1 The application will be centrally located at the data centre and will be accessible through fiber MPLS/ VSAT network of ICG.

238.2 Redundant Application Servers to provide load balancing and failover features.

238.3 The design of application should be modular as multiple modules can be integrated easily.

238.4 The interface design of the application should be simplified enough that end user can easily understand all the working. i.e. user friendly interface design.

238.5 The database should be configurable on high availability mode.

238.6 The database architecture should be simplified enough to provide faster results i.e. performance tuning.

238.7 The connectivity of database to the application should be local and with Gbps connectivity.

238.8 The application and databases at the ships can be deployed locally to control the local ships inventory.

238.9 The database of the ships synced with the central database when the ships integrated with the CG Chakra intranet network.

238.10 Proposed ERP application should be able to interface with existing ICG applications deployed on ICG middleware Platform 'SIMHA' such as ASHA, PARAM, BRASS etc for bi-directional data transfer without any licensing restrictions. Preferably, the application should expose key functions as web services for 3rd party interfacing and integration. The details may be given in technical bid for interface possibilities. Also, PARAM forms/ Gx, YATRA ICG portal can also be migrated to proposed ERP solutions. An integrated portal to view selected information should be developed on middleware platform 'SIMHA' as part of 'Unified ICG Portal' architecture requirements.

238.11 Functional and Non-functional requirement pertaining to integration of legacy application to proposed ERP solution will be discussed during the SRS stage.

239. **Militarized Zone/ Demilitarized Zone (DMZ)**.

239.1 **Militarised Zone**. The SAFAL Application being the core module proposed to be deployed in the secure zone and would have the most significant impact on the system with respect to resource requirements. Hence, it should be protected militarized zone in dual-firewall configuration.

239.2 **Demilitarised Zone (DMZ)**. The Network Centric applications in the servers to be deployed in the DMZ are as under:-

239.2.1 Web Services.

239.2.2 Directory Services.

240. **Licensing requirements**.

240.1 NUP mapped users may not be always available. In that case, NUP need to be transferred temporarily to other Users as required by Coast Guard.

240.2 NUP and any other type of license should be clearly mentioned for unit price. It will be required to calculate cost for future expansions.

240.3 Coast Guard to establish Service Oriented Architecture (SOA) as basic platform to achieve 'One Data' to prevent data in silos. Hence, Coast Guard may develop web services on ERP for integration with Coast Guard Office Automation Middleware platform (ICG SIMHA Platform) as required without any licensing implications.

240.4 Software licensing and relevant hardware architecture should be compliant to enterprise multi-hypervisor including VMware ESXi, Microsoft HyperV.

240.5 Should support by providing licenses as required for 'ERP Unlimited Data Exchange[1]' for any given ICG 'ERP Instance' with other ICG software systems such as 'ICG SIMHA' and BRASS etc.

240.6 Software licenses as required for 'ICG One Cloud' deployment of SAFAL ERP applications at ICG Ships & remote sites including DC & DRDC.

240.7 Software licenses should include project management related software such as MS Project Server, JIRA, Visual Paradigm or equivalent CASE (Computer Aided Software Engineering) tools native to OEM

241. **IT Infrastructure Characteristics Requirements**.

241.1 Should be built on enterprise support SDDC (Software Defined Data Centre) at all levels. SDDC to include SDC (Software Defined Computing), SDN (Software Defined Networking), SDS (Software Defined Storage)/ Unified Storage and SDSec (Software Defined Security).

241.2 Software Defined Security should have application, user & location awareness and implement micro-segmentation.

241.3 Should provide single-window, self-service portal to provision, deprovision of virtual computing, storage and networking.

241.4 Should provide virtualised 'Application Delivery Controller (ADC)' for application load-balancing, high-availability.

241.5 Should support enterprise multiple-hypervisor of including VMware vSphere ESXi, Microsoft Hyper-V and KVM.

241.6 Should supply, integrate required hardware along with licenses for Enterprise SDDC as certified by OEM of ERP.

241.7 Should provide storage based synchronous/ asynchronous replication.

241.8 Same SDDC infrastructure will be shared for other ICG software applications and the SI should provide necessary support at infrastructure level.

241.9 Computing, storage, networking, security products should be mentioned in latest Gartner Report.

241.10 All computing, storage and networking should be single OEM to provide native integration support between storage/ network/ computing, integrated management, single-point-of-support, and SDDC integration with OpenStack.

241.11 Hardware OEM should have direct service Centre at least at metro cities of Chennai, Mumbai, Delhi and Kolkatta.

241.12 Should supply, integrate SDDC software as certified by hardware OEM and integrate all supplied SDDC enabled hardware for single-window management.

241.13 Should provide required hardware, software licenses for Data Centre and DR Data Centre.

241.14 Primary storage should be all-flash including DAS and SAN.

241.15 Should have 'Disk to Disk to Tape' backup methodology at Data Centre & DR Data Centre and should use backup software to implement DDT along with required licenses.

241.16 Technical specifications of ERP hardware would be as contained in the preceeding sections of this Appendix.

242. **Sizing**.

242.1 Hardware sizing should be certified by ERP OEM.

242.2 Should be built on enterprise support SDDC (Software Defined Data Centre) at all levels. SDDC to include SDC (Software Defined Computing), SDN (Software Defined Networking), SDS (Software Defined Storage)/ Unified Storage and SDSec (Software Defined Security).

242.3 The specifications provided here under are indicative in nature for the purposes of selecting the hardware and services vendor. The final configuration of the servers would be determined in accordance with the requirement for the proposed ERP solution.

242.4 The seller should propose the bill of materials such that the technology, make, model, family of products implemented at Project site is in conformity with the specifications. It may be noted that the size and the capacity of individual components may vary depending on the requirements at each of the site and sizing need to be specified accordingly.

242.5 Support for data exchange through replicated database using data diode.

242.6 SAFAL ERP likely to be deployed secured militarized network. However, certain data need to be shared to internet based unified website through dedicated database.

242.7 Replication should be natively supported at database level.

243. **Application Lifecycle Management (ALM) Portal**.

243.1 Vendor should provide dedicated user accounts on ALM portal for Coast Guard.

243.2 ALM portal should manage all non-COTS related customizations & development.

243.3 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.

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

244.1 SAFAL ERP should support IAM and enable staff on-boarding feature.

244.2 Support IAM from Oracle as part of ICG SIMHA.

244.3 All roles should be exposed to IAM for centralised user management.

244.4 GRC should be implemented in the proposed ERP solution.

245. **Provisioning/ De-provisioning, Maintenance, DevOps as SaaS for ERP at Central & ROBO sites**.

245.1 ERP software should be provisioned/ de-provisioned as Self-service using SaaS software/ through tools, processes and procedures.

245.2 ERP to be deployed with single-click automation to DC, DR and ZT-ROBO Units connected over MPLS/ VSAT links/ through tools, processes and procedures.

MANPOWER, TRAINING & DOCUMENTATION REQUIREMENTS

Introduction

246. Managing and operating a Data Centre comprises a wide variety of activities, including the maintenance of all the equipment and systems in the data Centre, housekeeping, training, and capacity management for space power and cooling. These functions have one requirement in common, i.e. the need for trained personnel. As a result, an ineffective staffing model can impair overall availability.

Management and Operations

247. Management and Operations includes the behaviours that are most easily changed and have the greatest effect on the day-to-day operations of Data Centre. Management and Operations comprises behaviours associated with:-

247.1 Staffing and organization.

247.2 Maintenance.

247.3 Training.

247.4 Planning, coordination, and management.

247.5 Operating conditions.

Staffing

248. All the Management and Operations behaviours are important to the successful and reliable operation of a data Centre, but staffing provides the foundation for all the others. Data Centre staffing encompasses the three main groups that support the data Centre, Facility, IT, and Security Operations. Facility operations staff addresses management, building operations, and engineering and administrative support. Shift presence, maintenance, and vendor support are the areas that support the daily activities that can affect data Centre availability. Important attributes of staffing are as under:-

248.1 The number of personnel needed to meet the workload requirements for specific maintenance activities and shift presence.

248.2 The licenses, experience, and technical training required to properly maintain and operate the installed infrastructure.

248.3 The reporting chain for escalating issues or concerns, with roles and responsibilities defined for each group.

Factors to be considered for Staffing Requirements

249. In order to be fully effective, Data Centre staffing must comprise proper number of qualified personnel organized in correct manner. Many Data Centres are less than fully

effective because their staffing plan does not address these aspects. Apart from the management and operations, the staffing requirements also need to cater for various maintenance aspects (preventive maintenance, corrective maintenance, vendor support, project support etc.). In order to determine the staffing requirements, the number of hours for each activity attributed to each trade must be determined. For instance, the data Centre must determine what level of shift presence is required to support its business objective.

250. As uptime objectives increase so do staffing presence requirements. Besides deciding whether personnel is needed on site 24x7 or some lesser level, the data Centre operator must also decide what level of technical expertise or trade is needed. These decisions make it possible to determine the number of people and hours required to support shift presence for the year. Activities performed on shift include conducting rounds, monitoring the building management system (BMS), operating equipment, and responding to alarms. These jobs do not typically require all the hours allotted to a shift, so other maintenance activities can be assigned during that shift, which will reduce the overall total number of staffing hours required.

251. Once the total number hours required by trade for maintenance and shift presence has been determined, it is to be divide by the number of productive hours (hours/person/year available to perform work) to get the required number of personnel for each trade.

252. Data Centre personnel also need to be technically qualified to perform their assigned activities. As the Tier level or complexity of the data Centre increases, the qualification levels for the technicians also increase. They all need to have the required licenses for their trades and job description as well as the appropriate experience with data Centre operations.

Manpower Requirements

253. Manpower plays a vital role to sustain the entire system to deliver intended results. Considering the uptime requirements specified in the earlier parts of this DPR, it is imperative, that the Data Centre, Near DC, DR Data Centre, Networking & core IT software such as SAFAL ERP need to be provided centralised support by the SI on 24 x 7 x 365 basis for the entire life cycle of the project. In consideration of the factors brought out in the preceding paras, requirement of following technical manpower is recommended for duration of 05 years: -

253.1 **Onsite manpower support for Data Centre**.

SERVICES - AMC/ MANPOWER SUPPORT Manpower, IT Infra & Cloud			
253.1.1	Cloud automation, L2, OEM provided	1	No.
253.1.2	Virtualisation support, L2	1	No.
253.1.3	Network Engineer for NOC, L2, 24x7	1	Set
253.1.4	ITOM, ITSM & APM Support, L2	1	No.
253.1.5	Server, Storage, Backup, 24x7	1	Set
253.1.6	Linux Administrator, L2	1	No.
Manpower, SOC			
253.1.7|	Security Analyst, L2	2	Set
SERVICES - NON-ICT AMC/ MANPOWER SUPPORT			

VERIFIED

Manpower, Non-ICT			
253.1.8	Data Centre Facility cooling, power & floor management, L1, 24x7	1	No.
253.1.9	Data Centre Facility cooling, power & floor management, L2	1	No.
253.1.10	DCIM, IBMS Support, L2, 24x7	1	No.
253.1.11	Fire Prevention & Protection Officer, L2	1	No.
253.1.12	Service Desk Support Engineer, 24x7	1	No.
253.1.13	Support for L2, L3 offsite manpower, Facility Management	5	Yrs

253.2. **Onsite manpower support for Disaster Recovery Data Centre**.

SERVICES - AMC/ MANPOWER SUPPORT			
Manpower, IT Infra & Cloud			
253.2.1	Virtualisation support, L2	1	No.
253.2.2	Network Engineer for NOC, L2, 24x7	1	Set
253.2.3	Server, Storage, Backup, 24x7	1	Set
253.2.4	Linux Administrator, L2	1	No.
Manpower, SOC			
253.2.5	Security Analyst, L2	2	Set
General			
253.2.6	SI Services, One-Time	1	No
253.2.7	SI Services, Recurring	1	No
SERVICES - NON-ICT AMC/ MANPOWER SUPPORT			
Manpower, Non-ICT			
253.2.8	Data Centre Facility cooling, power & floor management, L1, 24x7	1	No.
253.2.9	Data Centre Facility cooling, power & floor management, L2	1	No.
253.2.10	Support for L2, L3 offsite manpower, Facility Management	5	Yrs

254. **Support Level & Exit Management for DC and DRDC**

254.1 L2 support engineers shall be OEM certified and having minimum experience of 03 year. All L2 engineers shall be able to maintain the system independently. Issues not resolved by L2 shall be escalated to OEM support being L3.

254.2 L1 support engineers shall be a combination of ICG service personnel and SI/ OEM manpower initially trained by specialist L2 engineers as on-job training.

254.3 L3 support shall be provided from OEM for Cloud Automation/ Orchestration/ SDDC Software, Enterprise Management System, NGFW software, SD-WAN and Data Centre SD-Network. SI should obtain dedicated support of minimum 100 hours per year extendable as required (or) any other suitable support, so as to ensure all raised tickets on each of mentioned items/ services are resolved with assured SLA by SI. SI should position a dedicated L2 level support engineer from OEM for Cloud Automation/ Orchestration/ SDDC.

254.4 Onsite/ offsite manpower and support be provided as required to meet SLA.

Manpower Requirement for SAFAL ERP.

255. Following technical manpower will be required for duration of 05 years:-

Sl	Skill Area	Location	Qty	Skill Level
255.1	Functional ERP consultant (L3 level engineer with 05 years' experience, OEM certified), 03 Nos.	DC & DR	2 at DC 1 at DR	L3 at DC L3 at DR
255.2	Onsite ERP support engineers, OEM Certified, 03 years' experience, 06 Nos.	DC & DR	4 at DC 2 at DR	L2 at DC L2 at DR
255.3	Onsite ERP Database Administrator, OEM Certified, 03 years' experience, 02 No.	DC & DR	02	L2 at DC
255.4	Onsite ERP system engineer (02 Nos.), Middleware & Cloud Automation (02 Nos.) OEM Certified, 03 years' experience	DC & DR	3 at DC 1 at DR	L2 at DC

256. **Support Level & Exit Management for ERP**

256.1 All ERP support engineers shall be OEM certified and having minimum experience of 03 year.

256.2 All L2 engineers shall be able to maintain the system independently. Issues not resolved by L2 shall be escalated to OEM. Vendor to provide 01 certified support engineer each on ICG SIMHA middleware platform/ unified and SIMHA portal developer. Cloud Automation support to have required skillset to configure/ develop scripts for provisioning/ deprovisioning, upgradation, DevOps of ERP Instance at DC, DR & ROBO and should be OEM certified.

256.3 Enterprise DBA be OEM certified with minimum of 03 years' experience in similar field.

256.4 L1 support engineers shall be ICG service personnel initially trained by specialist L2 engineers as on-job training.

256.5 As part of exit management, Bidder shall train ICG personnel to maintain the system end-to-end on completion of warranty/ AMC engagement.

Training Requirements

257. Training for all identified staff to be conducted for various roles of administration, support (L1/L2) of Main Data Centre, DR Data Centre, Networking and SAFAL ERP users to enable them to effectively operate and perform the relevant services using the software. The training content will have to be relevant to the target trainees depending upon the role. This training shall be designed to give the operators and maintainers (L1 & L2) necessary knowledge and skills to operate & maintain-Data Centre, Disaster Recovery Data Centre, SAFAL ERP Package and associated hardware The syllabus of the training should be defined by the Bidder in consultation with the Buyer at least six months prior offering the system for acceptance/ expiry of the delivery timeline. All training requirements such as training aids, projection system, complete equipment with accessories/ optional, technical literature as per ***Annexure-II*** *of* ***Appendix F***, spares, test equipment/ test set up, charts, training handouts, power point presentations, Computer Based Training (CBT), Documentation, Simulators etc. will be catered by the Bidder. Requirement of training aggregate is given at ***Annexure-III*** *of* ***Appendix F.***

Documentation Requirements

258. The bidder will provide detailed final system documentation for reference of ICG. System Integrator shall prepare the final user manual incorporating all details of all menus and functionality provided by the system. Indian Coast Guard expects the following (not limited to) in the form of product documents. In addition, the bidder will provide ongoing product information for reference purposes and facilitating self-education for ICG personnel. Key documents required are:-

258.1 Technical manuals.

258.2 Installation guides.

258.3 On-line help.

258.4 System administrator manuals.

258.5 Toolkit guides and Troubleshooting guides.

258.6 Configuration Documentation consisting of system settings and parameters for each function modules.

258.7 User Manual including system instruction and use cases, running of a program to perform specific task in the system with sample reports, screen formats etc.

258.8 Program flow and description.

258.9 Any other documentation required for usage of implemented solution.

258.10 System operational procedure manuals.

258.11 The bidder shall provide minimum three hard copies and two soft copies on (two different CDs) of the above mentioned manuals.

INFORMATION SECURITY REQUIREMENTS

259. Information Security Requirements required to be complied by the bidder are placed at ***Annexure-III*** to this Appendix.

VERIFIED

Annexure-I to Appendix 'A'
(Refers to Para 4(a) of Covering letter and Para 3.9 of this Appendix)

DETAILS OF EXISITNG HARDWARE/ SOFTWARE REQUIRED TO BE INTEGRATED

Sl.	Product	Description	Qty
1.	VMware vSphere 6	Resource Management, High Availability and Certificate Management	30 licenses (per processor based licensing)
2.	VMware-vCentre Server	Software to manage hosts and VMs centrally	02 Licences
3.	VMware NSX	NFV module	30 licenses (per processor based licensing)
4.	VMware SRM	Replicate VM Data	2 packs of 25
5.	Anti-Malware Server+ Clients	TrendMicro Smart Protection Complete	3 Servers with XXX CALs
6.	HIPS Server+ Clients	TrendMicro Deep Security Enterprise	3 Servers with 453 CALs
7.	Patch Management Server	Microsoft systems Centre	3
8.	Enterprise Backup Solution	Veritas Netbackup platform base	1
9.	Server Enclosures	HPE C3000	02 (DC)
10.	Sever Enclosure Ethernet Blade Switch	HPE 6125G	04 (DC-02 and DR-02)
11.	Blade Server	HPE BL460C G8	16 (DC-08 and DR-08)
12.	Blade Server	HPE BL460C 69	04 (DR)
13.	Store Once Backup Appliance	HPE Store Once 3540	01 (DC) 12 X 4 TB SAS
14.	SAN controller with file persona	HPE 3PAR 8400,20TB	02 (01 DC and 01 DR)
15.	NAS Service Processor	Proliant DL 120 G9	02 (01 DC and DR each)
16.	Tape Library	HPE LT07- HPE MSL4048	02 (01 DC and 01 DR)
17.	SAN Switch	HPE SN3000B	04 (DC-02 and DR-02)

VERIFIED

Sl.	Product	Description	Qty
18.	Data Centre Modular Rack	Rittal SK009	01 (DC)
19.	Modular Rack	CMC	01 (DC)
20.	IP Camera	Dahua DH-SD6C120T-HN	01 (DC)
21.	2 KVA UPS Online	EATON 9PX 11000	02 (DC)
22.	Server Enclosure/Chasis	HPE C7000	01 (DC)
23.	Server Encl C7000 SAN Switch	Brocade 8GB SAN Switch	02 (DC)
24.	Fiber Channel 16Gb 4 Port HBA	HPE FC HBA 16Gb	02 (DR)
25.	Fiber Channel 16Gb 2 Port HBA	HPE FC HBA 8Gb	01 (DR)
26.	HPE 3PAR StoreServ Fle Ctl v3 Sys	HPE 3PAR Storeserv (File persona)	01 (DR)
27.	HPE Ethernet 1G 4P 331FLR Adapter	HPE Ethernet 1G 4P 331FLR Adapter	01 (DR)
28.	HPE Ethernet 10Gb 2P 560SFP +Adapter	HPE Ethernet 10Gb 2P 560SFP+Adptr	01 (DR)
29.	L3 Switch 4-1G/10G, 24GE,4-10G	HPE Aruba 2930	02 (DR)
30.	UPS 2KVA	EATON, PW9130i2000R-XL2U	02 (DR)
31.	Rack Server (In DR)	Dell, Power Edge EMC R440	2x 12 core
		Dell, Power Edge EMC R740	2 x 20 core
		HPE DL380 Gen10	2 x 14 core
		HPE DL380 Gen09	04 x 16 core
32.	HPE Synergy, Composable IT Infrastructure Server Hardware	HPE Synergy	01 (DR)
33.	UTM Device	Fortinet, Fortigate 200E	02 (DR)
34.	SAN Switch for Server Enclosure	HP Brocade 8Gbps,8P	02 (DR)
35.	SAN Storage	3PAR Store Serv 7400	01 (DR)
36.	Service Processor 3PAR 7400	Proliant DL320 E Gen8	01 (DR)
37.	File Controller	3 PAR Store Serv 700	01 (DR)

VERIFIED

Annexure-II to Appendix 'A'
(Refer to Para 4(b) of Covering letter and
Para 3.9 of this Appendix)

DETAILS OF EXISTING APPLICATIONS TO BE INTEGRATED TO ERP SOLUTIONS

Sl.	Application	Description	Technology Stack
1.	CG-Yatra	Application facilitates online submission and auditing of TA/DA and LTC advances.	SOA micro services, J2EE app server (Tomcat), Spring 5.2.7, Oracle dB 12C, Hibernate, Java, Angular, HTML5, CSS
2.	ASHA	Automation of Service Health Care Administration (ASHA), automate and digitise the medical/ health care domain of ICG.	Java, Spring and Hibernate Framework, Restful Web Services, Oracle Service Bus. Java Script, jQuery, Oracle and Postgre Sql
3.	Pay and Allowances Records Auditing Management (PARAM)	PARAM provides complete automation of pay roll process of ICG i.e. from creation of Gx to generation of Statement of Entitlement.	SAP DMS Server 4.6, Windows Server 2012 R2, JBoss Wildfly 22.0, Weblogic Server 12C, Tomcat 9.0, PostgreSQL Community Edn 9.6, Java Spring Framework 4.0, Spring Boot 2.0, Angular Js, Angular 5, HTML5, CSS3.2, REST
4.	DMS-DR	Document Management System - Document Repository - provide common documents such as CGOs, Policies of CGHQ/ CGC/ RHQ/ DHQs, CGBRs, various reference manuals, routine e-magazines such as CGSMA Bulletins to all ICG Units including island units, ICG Ships with offline access.	JBoss widfly, PostgreSQL Community Edition 9.6, Eclipse 4.12, Java, Spring Framework 4.0, Spring Boot 2.0, Angular 5, JBoss Fuse, Keycloak 9.02, Entire Open JDK 8, Apache Maven 3.6.0, JenKins 2.204, Rundeck 3.026, HTML5, CSS 3.2

VERIFIED

Annexure-III to Appendix 'A'
(Refers to Para 33 of RFP and para 259 of this Appendix)

INFORMATION SECURITY REQUIREMENTS

Introduction

1. The Digital Coast Guard project is a very complex and ICT intensive project requiring integration of hardware, software, licences and network elements sources from various OEMs/ network service providers. Therefore, it is imperative that necessary mechanisms, checks and measures are instituted to address any deliberate of inadvertent information security vulnerabilities.

Mandatory Measures

2. In order to ensure mitigation of cyber/ information security threats, details of all the active components in the equipment being supplied along with their origin (i.e., OEM and country/ place of manufacture) are to be provided by the Bidders. From a cyber-security threat perspective, Systems and ICT hardware can be broadly categorized as follows:-

2.1. **Inert Components**. Which have no electronic circuitry like power & other cables, connectors, racks, chassis hardware etc.

2.2. **Passive Components**. Sub-systems/ PCBs which have electronic circuitry, but no intelligence in terms of software/ firmware/ microcode like backplanes, keyboard, mouse, monitor, normal printer etc.

2.3. **Active Components**. Sub systems/ PCBs which have device-specific intelligence that is built into firmware/ microcode like controller cards, hard disk drives, intelligent printers with smart features and memory, motherboards server management modules etc.

2.4. **High Active Components**. Appliances with a high level of intelligence built into firmware/ microcode, embedded OS & software.

3. Mandatory Security Audit & VA (Vulnerability Analysis) of the Hardware, ERP Application etc. by CERT-IN empanelled firms is recommended. To avoid "Malware and Malicious code attack" Bidder, OEM and supplier to provide a certificate stating that all known security issues and malware have been addressed in the products including hardware/ firmware/software and product is free from malware and malicious code at the time of supplying the hardware/ software products. Further, the Hardware/ Software should be from

the trusted OEM. Also Bidders to mention the country of origin of the product and provide following information:-

3.1. List of changes being made to Operating System due to software installation.

3.2. List of dependencies including software components and its DLL files.

3.3. List of processes including 'child processes' and service/ daemon being created in the Operating System.

3.4. Network Protocols and Ports being used by the product. In the event of custom protocols, complete description of the protocols is to be given.

3.5. Cryptographic Hash values of the files being provided.

3.6. A code Audit Certificate providing details regarding known exploit techniques (e.g. like buffer/ heap overflow), bugs, backdoors, list of components that could not be audited and Third party DLLs used.

3.7. Bidder need to carry out mandatory Security Audit & VA (Vulnerability Analysis) by CERT-IN empanelled firm of Hardware, ERP Application etc.

Additional Measures

4. The Bidders to list down all the measures taken by him to ensure that:-

4.1. No hostile actors insert a targeted subversion attack into the equipment.

4.2. The residual threats based on subversion of single components or subsystems, which may lead to shut down or partial loss of functionality, or to a series of privilege escalations leading to full-fledged control of the equipment.

4.3. Likely points of insertion of roots of trust and their effect on risk mitigation using well established security principles of containment, transaction control and confinement. Hence, insertion of roots of trusts into the equipment by the trusted system integrator may be employed to block the later type of attack and escalation.

4.4. Ensuring safety of the information assets from leakage and possible corruption or falsification.

4.5. Any other aspect to ensure Information Security.

4.6. Measures instituted by the Bidders to ensure that the equipment being supplied would be free of malicious code as confirmed by the Bidder in Malicious Code.

4.7. Measures taken to mitigate malware risks.

VERIFIED

4.8. Network Protocols and Ports being used by the product. In the event of custom protocols, complete description of the protocols is to be given.

4.9. Cryptographic Hash values of the files being provided.

4.10. A certificate stating "No known security issues, Malware, Trojans exist in the software components being provided".

4.11. A code Audit Certificate providing details regarding known exploit techniques (e.g. like buffer/ heap overflow), bugs, backdoors, list of components that could not be audited and Third party DLLs used.

4.12. Details of Active and High Active components are to be submitted as part of technical bids as per following format:-

DETAILS OF HIGH ACTIVE COMPONENTS

Sl.	Components	Qty	Country of Origin	Proposed Manufacturer(s)	Remarks

DETAILS OF ACTIVE COMPONENTS

Sl	Components	Qty	Country of Origin	Proposed Manufacturer(s)	Remarks

Appendix B
(Refers to Para 26, 30.2 and 31 of RFP)

COMPLIANCE TABLE

For Digital Coast Guard Project

Ser No	Requirement as per the RFP	Compliance/ Partial Compliance	Indicate references of Paras/ Sub Paras of the Main Technical Document
General Conditions of RFP (Para 01 to 25)			
Technical Parameters as per Appendix A			
1	Data Centre - civil infra as per Para 4 to 12 of Appendix 'A'		
2	Disaster Recovery Data Centre – civil infra as per Para 22 to 33 of Appendix 'A'		
3	Near Line Data Centre – civil infra as per Para 40 to 48 of Appendix 'A'		
4	ICT Components. - Compliance to be indicated in the table of Appendix 'A' from para 52 to 96.		
5	Network connectivity and component As per Para 100to 103 of Appendix		
6	ERP- As per Para 107 to 245 of Appendix 'A'		
Commercial Parameters as per RFP			
7	Performance-cum-Warranty Bank Guarantee as per Para **2** of **Appendix 'H'** RFP		
8	Advance Payment Bank Guarantee as per Para **1.3.8** of **Appendix 'H'** of RFP		
9	Earnest Money Deposit as per as per Para **8.2** of **Annexure to Appendix 'K'** of RFP (indicate amount of EMD)		

VERIFIED

Appendix C
(Refers to Para 12 & 34 of RFP and
Para 1 of Appendix 'F')

WARRANTY CLAUSE

1. The **SELLER** warrants that the goods/services supplied under this contract conform to technical specifications prescribed and shall perform according to the said Technical Specifications.

2. The Seller warrants for a period of **24** months from the date of installation and commissioning or final go-live, whichever is later, that the goods/ stores supplied under the contract (All civil work, DG sets, UPS & associated equipment, hardware and software installed at the Data Centre, Near Line Data Centre & Disaster recovery Data Centre including air-conditioning and power backup, hardware installed on-board ships, networking hardware, network links and the ERP package) and each component used in the manufacture thereof shall be free from all types of defects/ failures (including latent and patent defects).

3. If within the period of warranty, Data Centre, Near Line Data Centre, Disaster Recovery Data Centre, Coast Guard Wide Area Network and ERP Package/ modules/ hardware/ licenses 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, maximum within 24 hrs (for DC, NLDC and DRDC) and 07 working days for hardware supplied on-board ships of notification of such defect by the **BUYER** provided that the goods are used and maintained by the **BUYER** as per instructions contained in the Operating Manual. However, in no case, services supported by the Data Centre/ Disaster recovery Data Centre should be interrupted for more than 04 hours on each occasion. In case of hardware installed on-board ships, the **SELLER** shall either replace or rectify the same free of charge, maximum within 07 working days of notification of such defect by the **BUYER.** Warranty of the equipment would be extended by such duration **of downtime**. Record of the down time would be maintained by user in log book. In case of hardware installed on-board ships, the delay in replacement/ repairs beyond the specified period of 07 days due to non-availability of ships in harbor would not be counted as downtime. Spares **and all consumables** required for warranty repairs shall be provided free of cost by **SELLER**. In order to meet the warranty support requirement, the bidder will be required to maintain a minimum stock level of critical spares/ replaceable modules both at DC and DRDC. Similar stock levels for meeting the warranty requirements in respect of hardware installed on-board ships is to be maintained at a mutually agreed location so that the spare can be mobilized to the end user location to rectify the defect within 07 days. Time taken in shipment of spares from the mutually

agreed central site to end user locations will not be counted towards computation of downtime. The **SELLER** also warrants that the special oils and lubricants required for the warranty repair of the equipment shall be provided by the **SELLER** himself. **All activities including diagnosis, rectification, calibration, transportation etc, required for making equipment serviceable and available would be the SELLER's responsibility.** The **SELLER** also undertakes to diagnose, test, adjust, calibrate and repair/ replace the goods/ equipment arising due to accidents by neglect or misuse by the operator or damage due to transportation of the goods during the warranty period, at the cost mutually agreed to between the **BUYER** and the **SELLER**. The **SELLER** shall intimate the assignable cause of the failures.

4. **SELLER** hereby warrants that necessary service and repair backup during the warranty period, including routine maintenance beyond Unit Level shall be provided by the **SELLER** and he will ensure that the **cumulative** downtime **period for the** ERP Package/ modules/ hardware/ licenses **does not exceed 5% of the warranty period.** Downtime for the equipment/ facility will be calculated as per the SLA defined at ***Appendix 'F'.***

5. If a particular equipment/ goods fails frequently and/ or, the cumulative down time exceeds **5 %** of the warranty period **or a common defect is noticed** in more than **25**% of the quantity of goods with respect to a particular item/ component/ sub- component, module/ sub-module, that complete **item**/ equipment/ module/ sub-module shall be replaced free of cost by the **SELLER** within a stipulated period of **15 days** of receipt of the notification from the **BUYER** duly modified/ upgraded through design improvement in all equipment supplied/yet to be supplied and ESP supplied/yet to be supplied.

6. SELLER shall associate technical personnel of maintenance agency and QA of BUYER and OEM/ OEM certified agencies during warranty repair and shall provide complete details of defect, reasons and remedial actions for averting recurrence of such defects.

7. In case the complete delivery of the Warranty obligations is delayed beyond the period stipulated in this contract, then the **SELLER** undertakes that the warranty period for the goods/ stores shall be extended to that extent.

8. The SELLER warrants that the goods supplied will conform to the operating conditions and specifications as mentioned at ***Appendix A*** of RFP

9. During the period of warranty, the bidder would be required to routinely apprise the buyer on all updates, patches and upgrades through a periodic bulletin.

All updates and patches would be provided free of cost by the bidder to the buyer. Further, upgrades if any, warranting implementation during warranty period shall be the liability of the Bidder. During the period of warranty, the bidder would also be liable to comply with any other change request communicated by the Buyer, which otherwise do not fall within the purview of updates, patches or vendor recommended upgrades at a mutually agreed cost. For the purpose of this clause, update, patches and upgrades would be defined as under:-

9.1 **Update**. Updates means a modification, correction or addition to the software or documentation, including updates and enhancement for Current Products that the Vendor generally make available to its customers as a part of support and maintenance under a vendor support and maintenance agreement without additional charge. The definition of "Update" excludes Upgrades.

9.2 **Patch(es)**. Patches means additional programming code to be integrated with the Software to correct an error or alleviate its effects. It is a free set of changes to a computer program or it supporting data designed to update, fix or improve it. This includes fixing security vulnerabilities and other bugs, with such patches usually being called bug-fixes and improving the functionality, usability or performance.

9.3 **Upgrade**. Upgrade means an enhancement or addition to the Software other than an Update which the vendor does not make generally available to its customers as a part of support and maintenance under a vendor software support and maintenance agreement, but rather is only made commercially available for Current Products subject to payment of a separate incremental license fee, upgrade charge or as part of a subscription license fee.

10. The period of warranty would also include, complete defect liability of all civil infrastructure and associated facilities being created as part of the project.

Appendix D
{Refers to Para 32.1 of RFP}

PRELIMINARY PROJECT REPORT (PPR)

1. This PPR would broadly cover the following aspects: -

1.1 Project Overview.

1.2 Definition of key milestones based on indicative list of milestones and broad range of timelines specified at Para 45 of RFP.

1.3 Broad plan for execution of the Project as per delivery schedule indicated at Para 9 of Part-I of RFP.

1.4 Lifetime product support plan.

1.5 Plan for meeting the Indigenous Content (IC) stipulated in the RFP.

1.6 Standard of Preparation (SoP) of Platform/ equipment/ system.

1.7 Project organisation structure as applicable.

2. **Project Overview**. The *Project Overview'* should define, organise and interlink the various project elements which are required to be established/ setup by the Bidder and his- OEM partners/ sub-contractors in order to manufacture and deliver the contracted products and services within the RFP specified timeframes.

3. **Definition of Key Milestones**. This Annexure should define the key milestones in the project implementation phase and the criterion for declaring accomplishment of these milestones. The key milestones would include placement of orders on sub-contractors/ OEM partners/ service providers for civil works, hardware, software licences and network, certifications by uptime institute/ OEMs as specified in RFP, completion of civil works, delivery of hardware/ software, development of individual modules and complete ERP package, establishment of individual links and entire network, testing and evaluation of individual modules and complete ERP package and security audits as specified in the RFP.

4. **Program Schedule**. The *'Program Schedule'* should give **estimated start and end dates** for each event with respect to the award of contract (T0) thereby creating a **calendar-based schedule**.

5. **Standard of Preparation (SoP)**. Standard of Preparation (SoP) of the equipment/ system being offered must be defined in the PPR. This must include details of operational role-oriented equipment.

6. **Life Time Product Support Plan**. This document should bring out the Bidder's plan to provide product support throughout the Total technical Life (TTL) of the equipment/ system including obsolescence management plan, mechanism to incorporate various Support Contracts in future for repairs, mechanism to work out cost spares etc. for all future procurements by applying pre-defined escalation methodologies etc.

7. **Project Organisation Structure**. This section should highlight the Bidder's organisation structure for the project implementation and define the specific organisational elements within this structure that would interface with the GoI, SHQ and sub-contractors/ OEM partners/ service providers during the program execution.

8. **Any Other Issue That the Bidder Finds Relevant**. This section would include any issues that the Bidder finds relevant for the implementation of the 'Make' portion of the programme.

Appendix E
(Refers to Para 33 of RFP)

CERTIFICATE: MALICIOUS CODE

CERTIFICATE TO BE OBTAINED FROM OEM/ BIDDER FOR PROCUREMENT OF ICT GOODS AND SERVICES

(To be rendered on the Company Letter head)

1. This is to certify that the Hardware and the Software being offered as part of the contract does not contain embedded malicious code that would activate procedures to:-

1.1 Inhibit the desired and designed function of the equipment.

1.2 Cause physical damage to the user or the equipment during the exploitation.

1.3 Tap information resident or transient in the equipment/ networks.

2. The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Rights (IPRs) are caused due to activation of any such malicious code in embedded software.

3. The firm will provide the following malicious code certificates from Bidders and OEMs as given below to meet the project specific requirements and these may form part of the RFP and contract agreement.

(Signed)
Date: Designation/ Name/ Address of firm

MALICIOUS CODE CERTIFICATE FROM HARDWARE OEM

1. It is certified that the firmware/ microcode installed in the hardware products listed below, which is proposed to be delivered by our Business Partner M/s______, is approved by the OEM. The products have been thoroughly tested and found to be

working as per the OEM's specifications at the time of delivery and no malicious code has been found in these products. Patch level update of the system is enclosed.

2. The latest security patches as available at the time of supply, have been updated in the firmware. We undertake to provide solutions to address all security issues during the installation, warranty and support period of the equipment, provided end of support for the same has not been declared for the equipment by the OEM(s).

(Signed)
Date: Designation/ Name/ Address of firm

MALICIOUS CODE CERTIFICATE FROM SOFTWARE OEM

1. It is certified that the firm has taken all steps to ensure that the software products listed below, which is proposed to be licensed by _____ is found to be working as per the OEM's specifications at the time of delivery and no malicious software computer program/ code hidden within the software that performs a function unauthorized by the OEM's published documentation has been introduced in these products. Patch level update of the software is enclosed.

2. The latest security patches as available at the time of supply, have been updated in the software. We undertake to provide solutions to address all security issues during the installation, warranty and support period of the software, provided end of support for the same has not been declared for the equipment by the OEM's.

(Signed)
Date: Designation/ Name/ Address of firm

MALICIOUS CODE CERTIFICATE FROM BIDDER

1. This is to warrant that the hardware and software being offered, as part of the Contract does not contain embedded malicious code at the time of installation and commissioning. Patch level update of the hardware/ software is enclosed.

2. The firm will be considered to be in breach of the contract, in case any physical damage or any compromise in information and cyber security or infringement related

to copyright and Intellectual property Right (IPRs) is caused due to activation of any malicious code embedded in the hardware/software.

3. The latest security patches as available at the time of installation and commissioning, have been updated in the hardware/ software. We undertake to provide solutions to address all security issues during the warranty and support period of the hardware/software, provided end of support for the same has not been declared for the equipment by the OEM's and to address all exposed security issues by exercising immediate Work-around until the OEM has made the respective solutions available."

(Signed)
Designation/ Name/ Address of firm

Date:

Place:

Appendix F
(Refers to Para 34 of RFP and Para 4 of Appendix 'C')

PRODUCT SUPPORT

1. Product support and maintenance of the Core IT Infrastructure i.e. Data Centre, Disaster recovery Data Centre, Network links and components under CGWAN and ERP package SAFAL including associated hardware/ licenses would be provided through a comprehensive warranty for two years (As per ***Appendix 'C'***) followed by an All Inclusive Annual Maintenance Contract (AIAMC) for a period of three years (further extendable upto two years on mutually agreeable terms) post completion of two years warranty. The Bidder would be bound by a condition in the contract that he is in a position to provide product support for the software, licences, stores, assemblies/ sub-assemblies, spares and consumables, Special Maintenance Tools (SMT)/ Special Test Equipment (STE) subcontracted from other agencies/ manufacturer in terms of maintenance, materials and spares for a minimum period of seven years including warranty as per RFP after the acceptance of the project by the Buyer. Obsolescence Management would be integral to maintenance approach both during the warranty as well as AIAMC.

Warranty (to be read in conjunction with Appendix 'C')

2. During the period under warranty, the supplied goods/ stores/ services must conform to technical specifications prescribed and shall perform according to the said technical specifications. Further, the supplied goods/ stores/ services (all hardware and software installed at the Data Centre & Disaster recovery Data Centre including air conditioning and power backup, hardware installed on-board ships, networking hardware, network links and the ERP package) and each component used in the manufacture thereof shall remain free from all types of defects/ failures (including latent and patent defects).

3. If within the period of warranty, Data Centre, Disaster Recovery Data Centre, Coast Guard Wide Area Network and ERP Package/ modules/ hardware/ licenses fail to perform as per the specifications, they would be required to be either replaced or rectified free of cost, maximum within 24 hrs of notification of such defect provided that the goods are used and maintained as per instructions contained in the Operating Manual. However, in no case, services supported by the Data Centre/ Disaster recovery Data Centre should be interrupted for more than 04 hours on each occasion. In case of defects being reported in respect of hardware installed on-board ships, they should be either replaced or rectified free of charge, maximum within 07 working days of notification of such defect.

4. Warranty of the goods/ stores/ services reported to have been defective would be extended by such duration of downtime. Record of the down time would be maintained by user in log book. In case of hardware, installed on-board ships, the delay in replacement/ repairs beyond the specified period of 07 days due to non-availability of ships in harbor would not be counted as downtime. Spares and all consumables required for warranty repairs shall be provided free of cost. In order to meet the warranty support requirement, a minimum stock level of critical spares/ replaceable modules should preferably be required to be maintained at DC and DRDC. Similar stock levels for meeting the warranty requirements in respect of hardware installed on-board ships is to be maintained at a mutually agreed location so that the spare can be mobilized to the end user location within 07 days. Time taken in shipment of spares from the mutually agreed central site to end user locations will not be counted towards computation of downtime.

5. All activities including diagnosis, rectification, calibration, transportation etc. required for making equipment serviceable and available would be part of the warranty obligations. The warranty would also include diagnosis, testing, adjustment, calibration and repair/ replacement of goods/ equipment defects on which would have occurred due to accidents by neglect or misuse by the operator or damage due to transportation of the goods during the warranty period, at mutually agreed cost provided that the assignable cause of the failures is intimated and agreed upon. Necessary service and repair backup during the warranty period, including routine maintenance will also form part of warranty obligations and it has to be ensured that the cumulative downtime period does not exceed 5% of the total warranty period. Downtime for the equipment/ facility will be calculated as per the defined Service Level Agreement.

6. If a particular equipment/ goods fails frequently and/ or, the cumulative down time exceeds 5 % of the warranty period **or a common defect is noticed** in more than 25% of the quantity of goods with respect to a particular item/ component/ sub-component, module/ sub-module, that complete **item**/ equipment/ module/ sub-module shall be replaced free of cost within a stipulated period of 15 days of receipt of the notification from the **BUYER** duly modified/ upgraded through design improvement in all equipment supplied/ yet to be supplied and ESP supplied/ yet to be supplied. OEM/ OEM certified agencies must be closely associated while undertaking repair/ replacements of defective equipment during the warranty support period and complete details of defect, reasons and remedial actions for averting recurrence of such defects.

7. **All Inclusive Annual Maintenance Contract (AIAMC)**

7.1 Maintenance support beyond the warranty period of two years would be through an All-Inclusive Annual Maintenance Contract (AIAMC) for a period of Three (03) years. AIAMC services should cover the repair and maintenance of all the equipment and systems. The scope of AIAMC would cover all IT Infrastructure excluding civil works, Software, licenses and associated hardware of ERP, Annual Technical Support for ERP licences, required upgradation/ renewal of ERP and Database. Material assessment will be carried out during the fifth (05th) year post go- live. On the basis of the assessment report, AIAMC can be further extended for the duration of 02-03 years. However, any hardware and software requiring replacement will be procured by the buyer. The scope of AIAMC will include all upgrades/ updates/ integration of new technology into the existing/ original solution provided by the Seller. Software upgrades, bug-fixes/ patches will be provided by the Seller at no additional cost during the lifetime of the software.

7.2 The scope of work would also involve the following:-

7.2.1 **<u>Preventive Maintenance</u>.** A minimum of four Preventive Maintenance Service visits during a year (once every quarter) to the DC, DRDC and near DRDC to carry out functional check-ups and minor adjustments/ tuning as may be required.

7.2.2 **<u>Breakdown Maintenance</u>.** In addition to preventive maintenance, defect on Core IT Infrastructure, ERP package, associated Hardware, licenses and database as and when observed, will be required to be undertaken within 24 hrs from the reporting of the defect. However, **the total downtime of the data centres should not exceed 94.60 minutes in a year in order to maintain 99.982% of uptime commitment for tier-III data centres.** The system integrator has to provide a list of essential spares required to be maintained as onboard spares to ensure the obligatory uptime of data centres to ICG at least one month prior to the go-live date of the project. The spares can be maintained in a mutually agreed location so that it can be mobilised for breakdown maintenance within SLA with ease. The downtime of the equipment will commence from the time a defect is reported and the log of the same would be maintained.

7.2.3 **<u>Calibration</u>.** Periodic inspection and calibration services as set forth in the equipment manual shall be undertaken to ensure operational availability of the equipment. Requisite certificates may be rendered whenever major repairs/ maintenance on equipment is undertaken.

7.2.4 **<u>Software</u>.** Support for maintenance of the software (s) during the period of AIAMC would include the following:-

7.2.4.1 Upgrades, patches, fixes to the OS and the Application software.

7.2.4.2 Back-up and restoration of software, as and when required.

7.2.4.3 No malware certificate.

7.2.4.3 Version of the software and IV & V (Independent verification and validation) certificate as per the applicable CMM Level, depending on the criticality of the equipment.

7.2.4.4 Method of checking the health of the software and debugging methods.

8 The response time should not exceed 24 hours from the time of notification of the breakdown/ defect. **Serviceability of 99.982% per year is to be ensured**. Required spares to attain this serviceability may be stored at site by the bidder at his own cost. Total down time would be calculated at the end of the year.

9 In order to ensure timely product support, an Online Inventory Management System (OIMS) may be considered. The OIMS shall also provide feature to track the delivery status of the items. Further the OIMS should provide dashboard for intimation on obsolescence and offer of lifetime buy along with provision for user to interact with the OEM for technical assistance etc. The software must have a provision to insert/ delete/ update line items as installed/ commissioned in DC/ DRDC and notification for expiry of warranty of licence/ hardware must be part of single dashboard.

Obsolescence Management

10 The obsolescence management for the equipment delivered under the scope of contract would from part of both the warranty and AIAMC. The obsolescence management will include providing "Form, Fit and Function" replacement of any system/ sub system rendered obsolete during the period of Warranty and/ or AIAMC. A clearly defined methodology is therefore imperative to undertake Active Obsolescence Management through life cycle of equipment which would include upgradation of ERP application, licenses and hardware on completion of its fair service life. The obsolesce management philosophy must incorporate the modality for timely notification of likely technology obsolescence of various modules of ERP application, licenses and hardware. In case of impending obsolescence of components, alternate item or option for lifetime buy would also be required to be notified.

Service level Agreement

11 The product support during the period of AIAMC is to be provided as per the Service Leval Agreement to be included in the contract. Details are placed at **Annexure-I** to this **Appendix-F**.

Annexure I to Appendix F
(Refers to Para 11 of this Appendix)

TERMS & CONDITIONS TO BE FOLLOWED DURING THE PERIOD OF WARRANTY AND AIAMC

1. The product support during the period of AIAMC is to be provided as per the Terms & Conditions to be included in the contract. Details are as under:-

1.1 The purpose of this Terms & Conditions is to clearly define the levels of service which shall be provided by the Service Integrator to ICG for the duration of this contract period of the Project.

1.2 Timelines specified in the above section (Work Completion Timelines and Payment Terms) shall form the Service Levels for delivery of Services specified there-in.

1.3 All the payments to the SI are linked to the compliance with the SLA metrics specified in this document.

1.4 The projected Terms & Conditions are proposed to be performance based. For purpose of Terms & Conditions, the definitions and terms as specified along with the following terms shall have the meanings set forth below:-

1.4.1 "Uptime" shall mean the time period for which the IT Infrastructure Solution along with specified services/ components with specified technical and service standards are available for users in all scope Applications across the DIT application landscape. Uptime, in percentage, of any component (Non IT and IT) can be calculated as: Uptime = {1- [(System Downtime)/ (Total Time - Planned Maintenance Time)]} * 100

1.4.2 "Downtime" shall mean the time period for which the IT Infrastructure Solution and/ or specified services/ components with specified technical and service standards are not available to users. This includes Servers, Routers, Firewall, Switches, all servers and any other IT and non-IT infrastructure, their subcomponents etc. at all Project locations etc. The planned maintenance time/ scheduled downtime will include activities like software upgrades, patch management, security software installations etc.

1.4.3 The selected SI will be required to schedule ‘planned maintenance time’ with prior approval of ICG. This will be planned outside working time. In exceptional circumstances, ICG may allow the SI to plan scheduled downtime in the working hours.

1.4.4 “Incident” refers to any event/ abnormalities in the functioning of the IT Infrastructure solution and services that may lead to disruption in normal operations.

1.4.5 “Helpdesk Support” shall mean the 24x7x365 centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.

1.4.6 “Response Time” shall mean the time incident is reported to the help desk and an engineer is assigned for the call.

1.4.7 “Resolution Time” shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the SI and conveying the same to the end user), the services related troubles during the first level escalation.

1.5 The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:-

1.5.1 Critical: Critical/ Central IT Infrastructure solution down impacting critical business functions or multiple modules/ functions down impacting users on daily operations or any module/ functionality deemed as highly critical by ICG .

1.5.2 High: IT Infrastructure solution down impacting critical business functions or multiple modules/ functions down impacting users on daily operations or any module/ functionality deemed as highly critical by ICG.

1.5.3 Medium: One module/ functionality down impacting critical business functions having major impact on daily operations.

1.5.4 Low: Loss of business functionality for less than 10 users impacting day to day operations or minor functionality down impacting less than 10 users.

1.6 The Terms & Conditions have been logically segregated in the following categories:-

1.6.1 Supply/ Installation/ Configuration of IT Infrastructure.

1.6.2 Uptime Measurement

1.6.3 Infrastructure SLA

1.6.4 Cloud Services Related Service Levels

1.6.5 MIS Reporting Service Levels

1.6.6 Help Desk related Levels

Commencement of Terms & Conditions: The Terms & Conditions shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the next payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

1.7 **Supply/ Installation and Configuration of IT Infrastructure**

Ser.	**Parameter**	**Metric**	**Basis**	**Penalty no.**
1.7.1	Adherence to planned implementation schedule. Detail project assessment report Project Initiation, User Acceptance Testing, Implementation, Stabilization, Operational Acceptance	The delay for each milestone as per the planned schedule should not exceed more than a week without a justified reason agreed and approved by ICG. Thereafter for each week of delay, penalty will be levied.	Per Occurrence	Rs 2 Lakh/week for the two weeks and Rs 5 Lakh for every subsequent weeks subject to a maximum of Rs 50 Lakh post which ICG may invoke annulment of the contract. The penalty will be levied for delay for reason attributable to the vendor.

1.7.2	Submission of deliverables as relevant to the individual milestones/stages Various deliverables such as • Inception Report • Survey Report • Project Plan • Quality Plan • Design Documents • SRS • Test Cases and results • User Manuals • Training Manual • Technical Documents etc.	To be submitted within 10 days of the completion of the individual milestone.	Per Occurrence	Rs 1 Lakh for the first week and Rs 2 Lakh for every subsequent week subject to a maximum of Rs 10 Lakh post which ICG may invoke annulment of the contract. The penalty will be levied for delay for reason attributable to the vendor.

1.8 **Uptime Measurement Method**

Ser	Parameter	Target	Measurement method
1.8.1	Overall Cloud Solution Availability	>=99.95%	Overall Cloud Solution Availability will be measured by following formula: Availability %age = {(Agreed Service Time - Subsystem Down Time) / (Agreed Service time)*(100%). Scheduled downtime will be excluded
1.8.2	Cloud Network Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)
1.8.3	Cloud Virtualization Layer Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)

1.8.4	Cloud Virtualization Layer Scalability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)
1.8.5	Cloud Storage Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)
1.8.6	Virtual Operating System Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)
1.8.7	Cloud Orchestration layer Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)
1.8.8	Cloud Security Layer Availability	>=99.95%	The component availability will be measured by following formula: Component Availability %age = {(Agreed Service Time for the component- Down Time of the component)/ (Agreed Service time for the component)*(100%)

1.9 **Infrastructure Related Terms & Conditions**

Ser.	Parameter	Target	Basis	Penalty
1.9.1	Power availability	>=99.75%	per occurrence	0.5% QP* per hour
1.9.2	PAC System availability	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP

1.9.3	PAC System availability would mean temperature and humidity at the rack level.	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.4	Temperature to be maintained 20°± 2° at all times	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.5	Relative humidity to be maintained 50°± 5° at all times	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.6	All individual Networking equipment availability including routers, switches	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.7	Connectivity with SWAN availability	>= 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.8	Internet Bandwidth availability	>=99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.9	LAN Availability	>=99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.10	Storage System	> = 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.11	CCTV System availability	> = 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP

1.9.12	Individual Camera availability	100% of the Cameras available	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.13	DVR system availability	> = 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.14	CCTV recording - 6 months from the time of recording	> = 99.75%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP
1.9.15	Fire Suppression and Detection System availability	> = 100%	per occurrence	99.25% - 99.75% - 1% of QP 98.75% - 99.25% - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP

* QP= Quarterly Payment

1.10 **Cloud Service Provisioning**

Ser	Parameter Target Basis Penalty	Target	Basis	Penalty
1.10.1	Provisioning and De-provisioning of Virtual Machines	Within 15 minutes	Per occurrence. This will be calculated monthly	0.5% of the QP for every 1 hours of delay beyond the target time. To the maximum capping of 5 hrs. Beyond 5 hours, 1% of the QP for every 1 hour.
1.10.2	Uptime of Cloud Resource supplied (server/VM etc) (including the Hypervisor, VM and OS running on it)	>= 99.95%	Per occurrence. This will be calculated monthly	
1.10.3	Uptime of Cloud Solution/ Applications/ websites	>= 99.95%	Per occurrence. This will be calculated monthly	99.25% - 99.95% - 1% of QP 98.75% - 99.25 % - 2% of QP Subsequently, every 0.5% drop in SLA criteria - 2% of QP

VERIFIED

1.11 **MIS Reporting**

Definition	**Target**	**Penalties**
The SI shall submit the MIS reports as requested by the DIT, broadly classified below but not limited to: -IMAC (Install, Move, Add, Change) Report Exception report indicating calls Completed beyond SLA, with calculation of non-performance deduction.	Report for the previous quarter shall be submitted to the DIT by the 5th day of beginning of current quarter	< 5 Days- No Penalty Between - 10days - 0.5%of QP Between 11 - 20days - 1% of QP Between 21 - 30days - 2% of QP

1.12 The severity would be defined as follows:-

1.12.1 **<u>Critical</u>**: In case more than 1 physical servers are down threatening business continuity (VMs on the physical server are not accessible and not working and Multiple Clients are affected) which is attributable to the Cloud Solution implemented by the SI, it shall be considered as a Critical incident.

1.12.2 **<u>High</u>**: In case 1 physical server is down causing high impact on business operations (VMs on physical server are not accessible/not working (few clients are affected) which is attributable to the cloud solution implemented by SI.

1.12.3 **<u>Medium</u>**: In case an essential functionality of the Cloud solution (like VM availability) becomes unavailable in the Live Cloud environment which is not actually hampering the live services of the Cloud but may impact the services if not attended immediately will be termed as medium.

1.12.4 **<u>Low</u>**: The incidents would be termed as low, which does not have any significant impact on the Cloud service delivery (little or no impact on business entity), eg: A minor problem or question that does not affect the software function, An error in software product Documentation that has no significant effect on operations; or A suggestion for new features or software product enhancement.

Response Time: The response time for all Types of Help Desk services incidents shall be less than 15 min.

1.13 **Helpdesk Support/ Issue Response and Regulation**

Ser	Severity	Resolution Time	Basis	Penalty
1.13.1	Critical	<1 hour	Per Incident	No Penalty
1.13.2	Critical	Between 1 hour and 2 hours	Per Incident unresolved	0.5% of the QP for every unresolved call
1.13.3	Critical	Between 2 hour and 3 hours	Per Incident unresolved	1% of the QP for every unresolved call, up to 10% of QP
1.13.4	Critical	>3 hours	Per Incident unresolved	2% of the QP for every unresolved call, up to 10% of QP
1.13.5	High	<1.5 hour	Per Incident	No Penalty
1.13.6	High	Between 1.5 hour and 2.5 hours	Per Incident unresolved	0.5% of the QP for every unresolved call
1.13.7	High	Between 2.5 hour and 3.5 hours	Per Incident unresolved	1% of the QP for every unresolved call, up to 10% of QP
1.13.8	High	>3.5 hours	Per Incident unresolved	2% of the QP for every unresolved call, up to 10% of QP
1.13.9	Medium	<2 hours	Per Incident	No Penalty
1.13.10	Medium	> 2 Hours and < 4 Hours	Per Incident unresolved	0.5% of the QP for every unresolved call
1.13.11	Medium	>4 hours	Per Incident unresolved	1% of the QP for every unresolved call, up to 10% of QP
1.13.12	Low	1 day from the time of incident logged at the help desk	Per Incident	No Penalty
1.13.13	Low	> 1 day and <5 days	Per Incident	0.5% of the QP for every unresolved call
1.13.14	Low	>5 days	Per Incident	1% of the QP for every unresolved call, up to 10% of QP

1.13.15	Average Call Lost Rate (Total No. Of calls lost because they were	<=1%	Per Month	0.1% of the QP for every additional 1% call lost subject to a maximum of 10% of QP

Note:

(i) The SI has to submit all the reports pertaining to SLA Review process within 2 weeks after the end of the quarter failing which TPA may consider the available data for creation of audit report.

(ii) All the reports must be made available to ICG, as and when the report is generated or as and when asked by the competent authority.

(iii) The down time will be calculated on monthly basis. Non-adherence to any of the services as mentioned below will lead to penalty as per the SLA clause and will be used to calculate downtime.

(iv) The total deduction per quarter shall not exceed 20% of the total QP value.

(v) Two consecutive quarterly deductions amounting to more than 20% of the QPs on account of any reasons will be deemed to be an event of default and termination

(vi) It is the right of the ICG to bring/deploy any external resources / agencies at any time for SLA review

(vii) The SI shall deploy sufficient manpower suitably qualified and experienced in shifts to meet the SLA. Agency shall appoint as many team members as deemed fit by them, to meet the time Schedule and SLA requirements.

1.14 Considering the complex nature advanced systems such as Cloud Management Platform, SD Networking, ITOM/ ITSM Software, SOC software such as SIEM etc., need specialised onsite manpower and also need back-to-back support of respective OEMs to get reliable support and optimum exploitation. SLA setup to be as following:-

1.14.1 **<u>Level-1 (L1) Support</u>**. For day-to-day onsite operations and maintenance. Support staff to have minimum of 02-03 years of experience. OEM Certification is preferred.

1.14.2 **Level-2 (L2) Support**. Any issues or need of new configurations/ setup, the services of L2 should be made available from OEM Certified engineers having adequate support experience.

1.14.3 **Level-3 (L3) Support**. Should be for escalation of services from L2 and should be handled by authorised OEM partners/ OEM and should be final stop for all DC related support & services. Bidder to position OEM manpower for Cloud management platform and for other support need get back-to-back OEM support including ITOM/ ITSM software, SOC software, PKI systems, APM software etc. for the entire support period of 05 years.

Annexure II to Appendix-F
(Refers to Para 16 of RFP & Para 257 of Appendix A)

TECHNICAL LITERATURE

The bidder will provide detailed final system documentation for reference of ICG. Bidder shall prepare the final user manual incorporating all details of all menus and functionality provided by the system. Indian Coast Guard expects the following (not limited to) in the form of product documents. In addition, the bidder will provide ongoing product information for reference purposes and facilitating self-education for ICG personnel. Key documents required are:-

EQUIPMENT: **Digital Coast Guard Project**

Original Equipment Manufacturer (OEM):-

Ser No.	Technical Literature	Unit Cost	Scale For equipment	Total Cost	Remarks
1.	User Handbook/operators Manual including system instruction and use cases, running of a program to perform specific task in the system with sample reports, screen formats etc.				
2.	Installation guides and System administrator manuals.				
3.	Technical Manual. (a) Part I. Tech description, specifications, functioning of various Systems. (b) Part II. Inspection/ Maintenance tasks, Repair procedures, materials used, fault diagnosis and use of Special Maintenance Tools (SMTs)/Special Test Equipment (STEs). (c) Part III. Procedure assembly/ disassembly, repair up to component level, safety precautions. (d) Part IV (i) Part list with drawing reference				

	(ii) List of SMTs/STEs				
4.	Toolkit guides and Troubleshooting guides.				
5.	Configuration Documentation consisting of system settings and parameters for each function modules.				
6.	System operational procedure				
7.	Program flow and description				
8.	On-line help				
9.	Any other				
10	CDs on the above Tech literature				

VERIFIED

Annexure-III to Appendix-F
(Refers to Para 16 of RFP and Para 257of Appendix-A)

TRAINING AGGREGATES

1. Training for all identified staff to be conducted for various roles of administration, support (L1/ L2) of Main Data Centre, DR Data Centre, Networking and SAFAL ERP users to enable them to effectively operate and perform the relevant services using the software. The training content will have to be relevant to the target trainees depending upon the role. This training shall be designed to give the operators and maintainers (L1 & L2) necessary knowledge and skills to operate & maintain-Data Centre, Disaster Recovery Data Centre, SAFAL ERP Package and associated hardware. The syllabus of the training should be defined by the Bidder in consultation with the Buyer at least six months prior offering the system for acceptance/ expiry of the delivery timeline. All training requirements such as training aids, projection system, complete equipment with accessories/ optional, technical literature, spares, test equipment/ test set up, charts, training handouts, power point presentations, Computer Based Training (CBT), Documentation, Simulators etc will be catered by the Bidder.

2. Following type of training would be required:-

2.1. **Core IT Infrastructure**.

2.1.1. **DC/ DRDC Training**. Facility management, server/ desktop virtualisation, backup, archive & recovery, Active Directory, Email System, etc.

2.1.2. **Networking**. MPLS Router configuration, fault finding, testing, monitoring, Network Management Systems etc.

2.1.3. **Email & Central Intranet Portal**. Training should include administrator, developer, and data entry operator level.

2.1.4. Training will be conducted in two batches. Details of training requirement for each batch is as under:-

Sl.	Type of training	Mode of training	Duration of training	No. of Trainees
2.1.4.1	Data Centre Operations	Classroom Instructions	02 weeks classroom	20

	(intranet)	and OJT	instructions followed by 02 weeks OJT	
2.1.4.2	Data Centre Operations (internet)			15
2.1.4.3	DRDC Operations			20
2.1.4.4	DRDC Operations			15
2.1.4.5	SOC Operations			20
2.1.4.6	Network Operations			20
2.1.4.7	Email System			25
2.1.4.8	Central Intranet Portal training			25

2.2. **ERP 'SAFAL' Training.**

2.2.1. **Initial ERP Product Training**. Initial training will provide to ERP core team members. The training would provide understanding of the ERP solution and its functionalities. The training will highlight the unique requirement of the proposed ERP solution.

2.2.2. **ERP Functional Training (End User)**. Functional training would be provided to all ERP users across ICG. This training would focus on user specific requirements and address the daily working and reporting requirement in the ERP solution. A refresher training of all the functions needs to be provided to update the knowledge of ERP solutions.

2.2.3. **Technical Training**. Technical training to be provided by OEM certified trainers to the technical team of Coast Guard. The training matrix is as follows:-

Sl.	Type of training	No of batch	No. of Personnel / Batch	Duration (Days)	Location
2.2.3.1	Initial ERP product training	01	10	5	At NCR and Mangalore
2.2.3.2	ERP core team training by OEM	01	10	10	At NCR/ Mangalore

Sl.	Type of training	No of batch	No. of Personnel / Batch	Duration (Days)	Location
2.2.3.3	Oracle database administration	01	10	10	At NCR/ Mangalore
2.2.3.4	ERP End user Training	10	20	03	At NCR, Mumbai, Kolkata, Gandhinagar, Goa, Port Blair and Chennai.

VERIFIED

Appendix G
(Refer to Para 37 of RFP)

TRIAL METHODOLOGY

1. **Introduction.** Successful implementation of the Digital Coast Guard project would entail a careful examination, testing and inspection of the equipment, components, licenses and system of all the hardware, software and civil works for their compliance with the laid down functional/ technical parameters and specifications at various stages as per the procedure defined in the succeeding paragraphs: -

2. **Production Testing**. Production testing shall mean those tests which are to be carried out during the process of production to ensure the desired quality of end product to be supplied. The production tests to be carried out at each stage of production shall be based on the OEMs standard quality assurance procedures. The production tests to be carried out shall be listed along with information such as sampling frequency, applicable standards, acceptance criteria etc. The production tests would normally not be witnessed by the Purchasers representatives. However, the Purchaser reserves the right to do so or inspect the production testing records. Modalities in this regard are to be included in the contract.

3. **Factory Acceptance Testing (FAT)**. FATs shall be conducted by the Bidder/ OEM on randomly selected samples from final material to be supplied (at least 10% of batch size). Factory acceptance testing shall be carried out on all items being supplied. Equipment shall not be shipped to the Purchaser until required factory tests are completed satisfactorily and all variances are resolved. Full test documentation shall be delivered to the Purchaser along with the delivery of the equipment. Purchaser reserves the right to ask the Bidder/ OEM to carry out FAT in his presence.

4. **Pre Dispatch Inspection (PDI) and Joint Receipt Inspection (JRI)**. Pre Dispatch Inspection (PDI) would be at the discretion of the Buyer. In addition, Joint Receipt Inspection (JRI) may also be carried out. If it is PDI, the Bidder should intimate at least 45 days prior to the day when the equipment is to be offered for PDI to enable Buyer's QA personnel to be available for inspection. All the expenses towards PDI will be borne by the Bidder. In case of rejection of Goods during PDI, re-PDI will be undertaken at Bidder's premises at Buyer's sole discretion. All expenses including transportation and accommodation of Buyer's PDI team will be borne by the Bidder. In the event of a failed PDI, the Bidder shall consult the Buyer for rescheduling re-PDI. In case of JRI, the representative of the Seller may be present

for inspection after the equipment reaches the concerned destination. The Seller would be informed of the date for JRI.

5. It shall be ensured that there are no repetition of QA tests in PDI and JRI. The JRI would normally be restricted to quantitative checks only, except where check proof is required to be carried out. In case PDI/ JRI are planned to be conducted by authorised Third Party Inspection (TPI) Agencies/ Buyers nominated QA agency, the same will be spelt out and the details included in the finalised ATP. QA of equipment will be carried out as per finalised ATP. For technical trials by QA agencies, the Bidder will arrange for requisite test facilities at OEM premises/ accredited laboratories for establishing conformance. The successful Bidder would also be required to provide those test facilities at OEM premises/ accredited laboratories for quality assurance, which are not available with QA agencies. Details of the same will be included in the finalized ATP. ATP will also lay down the tests to be carried out during PDI and JRI.

6. **Staging & Deployment**. Upon completion of Delivery and SAT, a Staging & Deployment setup will be required to be established at sites culminating into a production environment.

6.1. During this phase all hardware/software solutions will be installed, deployed and activities like Functional Requirement Schedule (FRS), Software Requirement Schedule (SRS), Design etc. will be carried out i.e typical stages of development, testing, staging and production will be followed as part of this phase.

6.2. This phase will culminate into a production environment followed by Software/ Hardware Acceptance Testing and Integrated Acceptance Testing in a production environment, as described below. Sample data for the validation process and testing shall be provided by the L-1 bidder and duly approved by the purchaser.

7. **Acceptance Tests (AT)**. Since the implementation of the project involves Software and Hardware components, different types of AT shall be conducted at different levels. The exact test plans for testing the technical specifications and functional requirements for each system/subsystem as part of AT shall be prepared by the bidder and duly approved by the Purchaser (ICG) during the Design phase. Following type of acceptance tests shall be conducted at different stages upto final commissioning and go-live of the project:-

7.1. **Site Acceptance Tests (SAT)**. Site Acceptance testing shall be carried out by ICG. An audit of the process, plan and results of the Acceptance Test carried out by the bidder/ OEMs may also be undertaken. ICG would issue certification of completion for which ICG shall verify availability of all the defined services as per the conditions enumerated in RFP. The DC/ DR DC sites would be tested for the following parameters during Final Acceptance Test:-

7.1.1. All hardware and software items must be installed at ICG sites as per the specification and scope of the RFP. Visual inspection of material shall be carried out to ascertain if any damages have occurred.

7.1.2. The bidder shall be required to demonstrate all the features / facilities/ functionalities as mentioned in the RFP All documentation generated during design, installation and commissioning phase shall be made available.

7.2. **Software Acceptance Test**. Software AT shall be conducted for each software component/ solution and shall include the following:-

7.2.1. Commissioning of OSS solution.

7.2.2. Commissioning of IAM and PKI solution.

7.2.3. Commissioning of Data Centre Cloud and Virtualization solution etc.

7.2.4. Commissioning of SOC Solution including integration with all security devices (including Data Centre security devices) and all event/ log generating devices in the entire network.

7.2.5. Commissioning of IBMS Solution.

7.2.6. Hardware AT shall be carried out separately for each phase of implementation.

7.3. **Software Testing Requirements**. Bidder should avail services of 3rd party certified Software Testing from reputed vendors. Each software release/ iteration should be reviewed & tested by 3rd party Software Testing Service Provider (STSP) prior to submitting software to ICG. The required Software Testing Services are as following: -

7.3.1. Design, review & implement ERP/ Custom software associated for following: -

7.3.1.1. **<u>Functional Testing</u>**. Include Smoke testing, Unit testing/ module testing, Integration testing, System testing, Regression/ sanity testing.

7.3.1.2. **<u>Performance Testing</u>**. Carryout Load Testing, Stress Testing, Scalability Testing, Stability Testing by simulating conditions specific to ICG such as Wide Area Network (WAN), VSAT links with latency upto 1800ms etc.

7.3.1.3. **<u>Security Testing</u>**. Carryout Penetration Testing including network services test, web application security test, clientside security test, remote access security test, integration testing with ICG Identity Access Management (IAM), ICG Security Operations Centre (SOC) integration through Security Information and Event Management (SIEM) software etc/ CERT-In empanelled vendor.

7.3.1.4. **<u>Usability Testing</u>**. Carryout tests on navigation & structure, workflows & scenarios, content accessibility to comply with WCAG Guidelines, Comply to ICG SDOT UI/ UX standards, Usability Heuristics for User Interface Design, Heuristic evaluation, Cognitive walkthrough etc.

7.3.2. Design, review & implement Testing Requirements as part of SRS, Blue Print & Software Release phases as relevant of specific ERP Out-of- the-Box (OOTB), ERP Configurations, ERP Customisation and non-ERP custom software as part of the project. Test methods and standards should be meeting or exceeding OEM standards of specific ERP of the project.

7.4. **<u>Automated Software Testing</u>**. ERP/ Custom applications should be tested through 'Automated Software Testing' for each release of software through Version/ Sprints during entire software release lifecycle. **Automated Software Testing is mandatory** for Functional (Smoke) Testing, UI Testing, Integration Testing and Regression Testing.

7.4.1. Defining key points of the project. Closely cooperating with the rest of the project team, testing engineers define sets of conditions that allow the team to start, postpone, resume or stop the testing process.

7.4.2. **<u>Test Analysis and Design</u>**. The testing team transforms checklists (test ideas) into test cases and test suites.

7.4.3. **Test Implementation**. The testing team runs test cases and timely provides the developers with the information on bugs and defects.

7.4.4. **Result Analysis and Accountability**. The testing team provides a test summary report describing the results of testing efforts and software quality overview throughout a given cycle.

7.4.5. Compliance to ICG Software Development and Overseeing Team (SDOT) standards of Business Analysis Report/ SRS Report Format, UI/ UX Standards, Software Development Standards.

7.4.6. Carryout User Acceptance Test (UAT) for each iteration of software delivery as per SRS Project Plan. Software delivery iteration includes each Version of software till final go-live and each Sprints within Version. Each Use Cases as part of UAT to be tested using UI Testing software such as Selenium through automated testing. Required Selenium/ equivalent software script should be designed, developed & maintained by STSP.

7.4.7. For each project iteration through Versions & Sprints:-

7.4.7.1. Create test documentation required by ISO/ IEC/ IEEE 29119-3:2013 to ensure systematic and complete test coverage and ensure full visibility of the project's activities. All the documents are revised regularly to stay up-to-date.

7.4.7.2. Apply proven testing techniques, tools and methodologies to perform different types of testing to meet and even exceed your expectations regarding quality.

7.5. **Hardware Acceptance Test**. Installation and commissioning of all hardware/equipment being supplied as part of IT and Non IT infrastructure at DC and DRDC. All parameters of HAT will be accessed by the ICG project team.

7.6. **Acceptance of Civil Infrastructure**. The civil infrastructure being created as part of the project would be accepted through a joint inspection post production of necessary certification from the UPTIME institute. Defect liability in respect of civil infrastructure will continue to remain with bidder during the warranty period of two years.

7.7. **Integrated Acceptance Test**. On completion of installation and integration for the various subsystems of the network, Integrated Acceptance

Testing will be undertaken by the reps of ICG. The acceptance certificate will be issued by ICG for release of payment after successful completion of AT as per the Payment Terms. The functional requirements and implementation of the private cloud for ICG will be fully integrated with the supplied and existing hardware/ software i.e., integration with manager of the hypervisor, Software Defined Network and storage, etc. The CMP (Cloud Management Platform) will be integrated with the existing Directory Services software and will create business group as per the requirements given by ICG.

8. **Commissioning of System**. The bidder shall be responsible to provide test/ measurement tools and testers for conducting various tests. The bidder shall be obligated to remove defects/ deficiencies pointed out by the Inspection Officers without any additional cost.

8.1. The bidder should describe in advance the tests and details of the process that will be adopted to demonstrate the correct working of the equipment supplied both individually and as an integrated system.

8.2. System testing schedules, formats for testing and commissioning reports and dissemination mechanism for such reports shall be drawn by the bidder in consultation with ICG.

8.3. Successful completion of Commissioning would need to be certified by ICG and operations shall commence only after approval of ICG.

8.4. The date on which the Final Acceptance certificate is issued shall be the deemed date of the successful commissioning of the DC and DR site. Any delay by the successful bidder in the performance of its contracted obligations shall render the successful bidder liable to the imposition of appropriate liquidated damages, unless agreed otherwise by the ICG.

8.5. At the time of Final Acceptance Test, warranties of all the products would be checked, warranty should be there as per tender. Supporting documents like OEM warranty/ support certificate/ letter etc. to be submitted from respective OEM

9. **Certification**. On completion of the entire installation process at both the locations/ sites the bidder is to subject the complete network (inclusive of all components) for Vulnerability Assessment, Penetration Testing and Risk Assessment which would form the certification process. The certification is to be conducted by a Security Auditing Organisation empanelled by CERT-IN. The cost for certification by this agency is to be borne by the bidder. Any fault, lacunae, strengthening recommended by this agency is to be incorporated by the bidder free of cost on the recommendations of the ICG.

10. For JRI of the supplied equipment, evaluation of individual modules of the ERP package and Final User Acceptance Trials of the entire project including, functional DC, DRDC, WAN and the ERP solution, Bidder would be required to submit a Draft Acceptance Test Procedure (ATP) at least one month before scheduled evaluation/ trials. The draft ATP submitted by the Bidder must include Quality Assurance Plans (QAP) as per OEM standards i.e. tests undertaken to assure quality and reliability and provide the Standard Acceptance Test Procedure (ATP). Based on the draft ATP, the ATP will be finalised by the Buyer. The Quality Assurance (QA) agency/ Board of Officers appointed by the Indian Coast Guard reserves the right to modify the ATP if necessary. ATP will also lay down the tests to be carried out during PDI and JRI. In case PDI/ JRI are planned to be conducted by authorised Third Party Inspection (TPI) Agencies/ Buyers nominated QA agency, the same will be spelt out and the details included in the finalised ATP. QA of equipment will be carried out as per finalised ATP. For technical trials by QA agencies, the Bidder will arrange for requisite test facilities at OEM premises/accredited laboratories for establishing conformance. The successful Bidder would also be required to provide those test facilities at OEM premises/ accredited laboratories for quality assurance, which are not available with QA agencies. Details of the same will be included in the finalized ATP.

Appendix H
(Refers to Para 51 of RFP)

COMMERCIAL CLAUSES

1. Payment Terms

1.1 INCOTERMS for Delivery

1.1.1 The delivery of goods will be based on Free on Road (FOR) to Data Centre, Disaster Recovery Data Centrre, District Headquarters and respective sites for network components under intimation to Coast Guard Store Deport, Mumbai. Thereafter the equipment would be installed and commissioned at designated ICG locations in India.

1.2 **Currency of Payment**. bidders should submit their bids in Indian Rupees.

1.3 Contract Price and Requirement of Bank Guarantees

1.3.1. **Total Contract Price**. The Total Contract Price will be the final price negotiated by CNC including taxes and duties applicable at the time of signing of Contract.

1.3.2 **Base Contract Price**. The Base Contract Price will be considered as Total Contract Price excluding taxes and duties applicable at the time of signing of Contract and excluding the Total Price of AIAMC, Manpower and Bandwidth Charges for CGWAN.

1.3.3 **Bank Guarantee(s)**. For the purpose of payment of Advances to the Bidder and submission of various Bank Guarantees by the Bidder i.e Advance Payment Bank Guarantee (APBG), Base Contract price will be considered. For Performance cum Warranty Bank Guarantee (PWBG), Total Contract Price including taxes and duties is to be considered.

1.3.4 For orders with AIAMC, an additional Performance Bank Guarantee (PBG) is to be submitted by the Bidder for which the Total Price of AIAMC for contracted duration will be considered.

1.3.5 All Bank Guarantee(s) requirements viz Advance Payment Bank Guarantee (APBG), Performance-cum-Warrantee Bank Guarantee (PWBG), Performance Bank Guarantee (PBG) for AIAMC

1.3.6. **Indian Bidder**. In case of Indian Bidders, the Bank Guarantee(s) shall be from any Indian Public or Private Scheduled Commercial Bank.

1.3.7. **Payment to Indian Bidders**. The schedule for payments will be based on the Buyers requirements, enumerated at succeeding Paragraphs. The summary of delivery schedule and payments to be made are specified at **Annexure V** to this **Appendix H**.

1.3.8. **Advance Payment**. Fifteen (15) % of the Base Contract Price shall be paid within thirty (30) days of submission of claim and a Bank Guarantee for the equivalent amount, subject to correction and acceptability of the documents submitted. The advance payment of fifteen (15) % of the base contract price will be paid in two part. In first part of payment ten (10)% of base contract price will be paid on signing of contract. In second part of payment five (5) % of base contract price will be paid on submission of Project report (PR) and Project PERT Chart within 30 days from the date of signing of contract. The prescribed format of the Advance Payment Bank Guarantee (APBG) is placed at ***Annexure I*** to this ***Appendix*** **H**. The Advance Payment Bank Guarantee (APBG) will deemed to be proportionately and automatically reduced until full extinction along with and prorate to value of each delivery, as evidenced by corresponding copy of document proving delivery and invoices of goods/services supplied/provided. The date of delivery would be reckoned from the date of release of Advance payment by the Buyer to the Seller (T_0), provided the Seller submits the documents mandated by the DAP for release of advance by the Buyer within 45 days of signing of contract. In the event of the Seller not submitting the said documents within 45 days of signing of contract, the period between the 45 day and actual submission of documents will be excluded from the actual date of advance payment to arrive at the delivery date. In case, no advance is to be paid, the date for reckoning date of delivery would be the date of signing of contract. This clause will not be applicable in cases where in Advance payment is released after FOPM is successfully validated. In such cases, date of accord of Bulk Production Clearance will be date for reckoning date of delivery.

1.3.9. **Document Required to be Submitted**. The bidder has to provide following document along with invoice for the claiming of payment for the respective milestones:-

1.3.9.1 Ink signed copy of Seller's bill.

1.3.9.2 Ink-signed copy of Commercial invoice.

1.3.9.3 The relevant Transport Receipt.

1.3.9.4 Inspection Acceptance Certificate of Buyer's QA agency demonstrating compliance with the technical specifications of the contract.

1.3.9.5 Packing List.

1.3.9.6 Certificate of Origin.

1.3.9.7 Claim for statutory and other levies to be supported with requisite documents/ GST invoice (with QR code, when made applicable)/ proof of payment, as applicable.

1.3.9.8 Exemption certificate for taxes/duties, if applicable.

1.3.9.9 Warranty certificate from the SELLER.

1.3.9.10 Work Completion Certificate.

1.3.10. **Stage-wise Payments**. Delivery Schedule and stage wise payment or Core IT Infrastructure network and SAFAL ERP is placed at **Annexure V** to this **Appendix H**.

1.3.10.1 For stages mentioned above, payments will be released based upon the Completion certificate for all activities mentioned therein given by Buyer's representative. For all milestone payments, Bank guarantee for same amount will have to be furnished by the Seller before release of payments. The bank guarantee submitted for earlier stage will be returned on submission of bank guarantee for subsequent stages.

1.3.11. **AIAMC Payments**. Post completion of warranty period, Quarterly payments for AIAMC will be made by PCDA/ CDA on submission of User clearance certificate through issue of cheque/ ECS.

1.3.12. **Payment of Taxes and Duties**. Payment of taxes, duties and statutory levies will be made on submission of requisite documentary proof to Paying authority. Reimbursement of taxes and duties will be as per rates and amounts indicated in the commercial bid/contract or as per actuals whichever is lower.

2. **Performance-cum-Warranty Bank Guarantee Clause**. A Performance-cum- Warranty Bank Guarantee (PWBG) of 3% of value of the Total Contract Price including taxes and duties would be furnished by the Bidder in the form of a Bank Guarantee to sequentially act as Performance Bank guarantee till the delivery and as Warranty Bank Guarantee on delivery. The PWBG shall be submitted by the Bidder within one month of signing of contract and shall be valid for a period, until three months beyond the warranty period, as specified in the RFP. If at any stage, the Performance Guarantee is invoked by the Buyer either in full or in part, the Bidder shall make good the shortfall in PWBG within 30 days by an additional Bank Guarantee for equivalent amount. In the event of failure to submit the required Bank Guarantee against invoked Performance Guarantee, equivalent amount will be withheld from the next stage payment till the shortfall in the Bank Guarantee is made good by the Bidder. The prescribed format of the Performance-cum-Warranty Bank Guarantee is placed at **Annexure II to this Appendix** H.

3. **Performance Bank Guarantee for AIAMC** *(where applicable).* The Bidder will be required to furnish a Performance Guarantee by the way of a Bank Guarantee of a sum equal to 3% of the Total Price of AIAMC for contracted duration prior to expiry/ return of the PWBG of the Main Contract. Performance Bank Guarantee should be valid for 03 months beyond the period of the AIAMC. The format of the Performance Bank Guarantee is to be as per **Annexure II** to this **Appendix H**.

4. **Indemnity Bond**. DPSUs/ JV with DPSUs/ PSUs/ Government Entity may furnish Indemnity Bonds instead of Bank Guarantees towards Advance Payment Bank Guarantee and Performance- cum-Warranty Bank Guarantee as given in **Annexure III to this Appendix H**.

5. **Inspection**. Pre Dispatch Inspection (PDI) would be at the discretion of the Buyer. In addition, Joint Receipt Inspection (JRI) may also be carried out. If it is PDI, the Bidder should intimate at least 45 days prior to the day when the equipment is to be offered for PDI to enable Buyer's QA personnel to be available for inspection. All the expenses towards PDI will be borne by the Bidder except transportation and accommodation of Buyer's PDI team, which will be deputed at Buyer' expense. In case of rejection of Goods during PDI, re-PDI will be undertaken at Bidder's premises at Buyer's sole discretion. All expenses including transportation and accommodation of Buyer's PDI team will be borne by the Bidder. Towards this, the expenses towards transportation and accommodation of Buyer's PDI team will be initially done by the Buyer and subsequently reimbursed by the Bidder either by remittance or by recovery from the Balance Payment/PWBG. In the event of a failed PDI, the Bidder shall consult the Buyer for rescheduling re-PDI. In case of JRI, the representative of the Seller may be present for inspection after the equipment reaches the concerned destination. The Seller would be informed of the date for JRI.

VERIFIED

6. **Liquidated Damages (LD)**. In the event of the Bidder's failure to submit the Documents, supply the stores/ goods, perform services, conduct trials, installation of equipment, training and MET as per schedule specified in this contract, the BUYER may, at his discretion withhold cost of the specific lot/batch or 1% of the Project cost, whichever is higher, until the completion of the contract. The BUYER may also deduct from the SELLER as agreed, liquidated damages to the sum of **1/100** of the **delay percentage** {Delay percentage = (Period of Delay in Delivery in Weeks) x 100 / (Delivery Period in weeks as per contract)} of the Base 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 contract price of the value of delayed stores/ services (Any extension given by the Buyer for delay attributable to Buyer or Force Majeure Clause to be factored in delivery period).

7. **Payment Deductions and Damages for Shortfalls in AIAMC Services *(where applicable)***. In case the cumulative downtime exceeds **1.6 (hours**) in the ~~(~~Year), payment will be deducted. The total downtime will be calculated at the end of the financial year and payments will be deducted from the payments due for the final quarter of the financial year. The total payments to be deducted will be calculated as follows:-

(a) Payments would be deducted on pro-rate basis for the duration, by which cumulative downtime exceeds __ (1.6 hours), as follows:-

(i) Per year AIAMC= 'X1 '

(ii) Period by which cumulative downtime exceeds the specified cumulative downtime, in days = 'Y1'

(Hi) Payment Deduction = 'Z1'

*Where Z1 = [(X1/ Number of hours in the year) * Y1]*

(b) In addition, damages would be deducted to the sum of 0.1% of the per annum AIAMC cost per day, for the duration, by which cumulative downtime exceeds the maximum permissible cumulative downtime per quarter/ half-year/ year, subject to the maximum value of this damages not being higher than 5% of the annual AIAMC cost.

8. **Denial Clause**. In case the delay in delivery is attributable to the Seller or a non-force majeure event, the Buyer may protect himself against extra expenditure during the extended period by stipulating a denial clause (over and above levy of LD) in the letter informing the Seller of extension of the delivery period. In the denial clause, any increase in statutory duties and/ or upward rise in prices due to the Price Variation Clause (PVC) and/ or any adverse fluctuation in foreign exchange are to be borne by the Seller during the extended delivery period, while the Buyer reserves his

right to get any benefit of downward revisions in statutory duties, PVC and foreign exchange rate. Thus, PVC, other variations and foreign exchange clauses operate only during the original delivery period. The format for extension of delivery period/ performance notice under the Denial clause is at **Annexure IV** to this ***Appendix*** **H**.

Annexure I to Appendix H
(Refers to Para 1.3.8 of this Appendix)

BANK GUARANTEE FORMAT FOR ADVANCE

To
The ________________
Ministry of _____________
Government of India
_____________ (complete postal address of the beneficiary)

1. "Whereas President of India represented by the ______Ministry of ________Government of India (hereinafter referred to as BUYER) have entered into a Contract No.________(No. of Contract), dated ___(Date of Contract) with M/s ______(Name of SELLER) (referred to as SELLER) and whereas according to the said Contract the BUYER has undertaken to make an advance payment of Rs.____ being payment of _____% of the total value of Rs/ US $/ Euro/ PS £/ Yen/ AUD/SGD ____ of the said Contract, against issuance of an advance guarantee by a bank."

2. We ________(indicate the name of the bank) do hereby undertake to pay the amounts due and payable under this guarantee without any demur, merely on a demand from the BUYER intimating that the SELLER is in breach of the Contractual obligations stipulated in the said Contract. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our total liability under this guarantee shall be restricted to an amount not exceeding Rs______.

3. We undertake to pay to the BUYER any money so demanded notwithstanding any dispute or disputes raised by the SELLER in any suit or proceedings pending before any Court or Tribunal relating thereto our liability under this present being absolute and unequivocal. The payment so made by us under this bond shall be valid discharge of our liability for payment there under and the SELLER shall have no claim against us for making such payment.

4. We, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Contract and that it shall continue to be enforceable till all the dues of the BUYER under or by virtue of the said Contract have been fully paid and its claims satisfied or discharged or till ________office / Department / Ministry of _____ certifies that the terms and conditions of the said Contract have been fully and properly carried out by the said SELLER and accordingly discharges this guarantee.

5. We, further agree with the BUYER that the BUYER shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Contract or to extend time of performance by the said SELLER from time to time or to postpone for any time or from time to time any of the powers exercisable by the BUYER against the said SELLER and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of any such variation, Amendment issued vide MoD ID No. 4(50)/D(Acq)/08 dated 20.06.2016 or extension being granted to the said SELLER or for any forbearance, act or omission on the part of the BUYER or indulgence by the BUYER to the said SELLER or by any such matter or thing whatsoever which under law relating to sureties would, but for this provision, have effect of so relieving us.

6. The amount of this guarantee will be progressively reduced by (percentage of advance) ______ of total value of each part shipment/services against the stage payment released by the BUYER for that shipment/services made by the SELLER and presentation to us of the payment documents.

7. This guarantee will not be discharged due to the change in the constitution of the bank or the BUYER/SELLER.

8. We, undertake not to revoke this guarantee during the currency except with the previous consent of the BUYER in writing.

9. Notwithstanding anything contained herein above:-

9.1 Our liability under this Guarantee shall not exceed Rs/ US $/Euro/PS £/Yen/AUD/SGD ______ (in words) _________________.

9.2 This Bank Guarantee shall remain valid until ________ (hereinafter the expiry date of this guarantee) the Bank Guarantee will cease to be valid after _____irrespective whether the Original Guarantee is returned to us or not.

9.3 We are liable to pay guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written demand or a claim in writing on or before ______(Expiry Date).

Dated the _____ day of ______ (month and year)
Place :
Signed and delivered by _______ (Name of the bank)

Through its authorised signatory
(Signature with seal)

VERIFIED

Annexure II to Appendix H (Refers
to Para 2 & 3 of this **Appendix**)

BANK GUARANTEE FORMAT FOR PERFORMANCE-CUM-WARRANTY

To
The ________________
Ministry of ____________
Government of India
______________ (complete postal address of the beneficiary)
Dear Sir,

1. Whereas President of India represented by the _______ Ministry of ______ , Government of India (hereinafter referred to as BUYER) have entered into a Contract No. __________ dated ______ (hereinafter referred to as the said Contract) with M/s. ______ (hereinafter referred to as the SELLER) for supply of goods as per Contract to the said BUYER and whereas the SELLER has undertaken to produce a bank guarantee amounting to Rs. which is 3% of the Total Contract Price (including taxes and duties) to cover 5% of Total Contract Price (including taxes and duties) each for Performance and Warranty in sequence, to secure its obligations towards Performance-cum- Warranty to the BUYERs.

2. We, the _______________ bank hereby expressly, irrevocably and unreservedly
undertake the guarantee as principal obligors on behalf the SELLER that, in the event that the BUYER declares to us that the amount claimed is due by way of loss or damage caused to or would be caused or suffered by the BUYER by reason of breach/failure to perform by the said SELLER of any of the terms and conditions in the Contract related to Performance and Warranty clauses, we will pay you, on demand and without demur, all and any sum up to {3% of Total Contract Price (including taxes and duties)}________Rupees/US $/Euro/PS £/Yen/AUD/SGD only at any instance under this Guarantee. Your written demand shall be conclusive evidence to us that such repayment is due under the terms of the said Contract. We shall not be entitled to ask
you to establish your claim or claims under this guarantee but will pay the same forthwith without any protest or demur. We undertake to effect payment upon receipt of such written demand.

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

4. We further agree that any such demand made by the BUYER on the Bank shall be conclusive, binding, absolute and unequivocal notwithstanding any difference or dispute or controversy that may exist or arise between you and the SELLER or any other person.

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

6. This Performance-cum-Warranty guarantee shall remain valid for a period until three months beyond the warranty period as specified in the Contract i.e. up to _____.

7. Subject to the terms of this Bank Guarantee, the issuing bank hereby irrevocably authorizes the beneficiary to draw the amount of up to Rs. _____{3% of Total Contract Price (including taxes and duties)} for breach/ failure to perform by the SELLER of any of the terms and conditions of the Contract related to performance and warranty clause. Partial drawings and multiple drawings under this Bank Guarantee are allowed within the above stated cumulative amount subject to each such drawing not exceeding 3% of the Total Contract Price (including taxes and duties) (Rs/ US $/Euro/PS £/Yen/AUD/SGD _______ only) (Mention BG amount) (Mention BG amount).

8. This guarantee shall be continuing guarantee and shall not be discharged by any change in the constitution of the Bank or in the constitution of M/s _______________

We undertake not to revoke this guarantee during the currency except with previous consent of BUYER in writing.

9. Notwithstanding anything contained herein above:-

9.1 Our liability under this Guarantee shall not exceed Rs/ US $/Euro/PS £/Yen/AUD/SGD _________ (Rupees ___________ only (in words)

9.2 This Bank Guarantee shall remain valid until 3 months from the date of expiry of warranty period of the Contract, i.e up to ________ (mention the date) which is 3 months after expiry of the warranty period and the BG shall cease to be valid after _______________ irrespective whether the Original Guarantee is returned to us or not.

9.2 We are liable to pay guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written demand or a claim in writing on or before ______________ (Expiry Date).

Dated the _______ day ________(month and year)

VERIFIED

Place:
Signed and delivered by ______ (name of the bank)

Through its authorised signatory
(Signature with seal)

Annexure III to Appendix H
(Refers to Para 4 of this Appendix)

INDEMNITY BOND FOR PERFORMANCE-CUM-WARRANTY

1. This deed made on this ______ day of ___ by M/s , a company registered under The Companies Act 2013 having its registered office at _______ and acting through its corporate office at_______hereinafter referred to as the "SELLER").

2. Whereas MoD, New Delhi acting on behalf of the President of India (hereinafter referred to as "BUYER") has placed a Contract No._______ dated ________.

3. And whereas, the SELLER has agreed to execute this Indemnity Bond for performance- cum-warranty on the terms and conditions appearing hereinafter.

4. It is hereby agreed and declared by the SELLER that:-

4.1 The SELLER shall duly and faithfully perform its obligation under the said contract and comply with the conditions in the said contract.

4.2 The SELLER shall, in as much as with its control, refrain from such actions or actions as may cause loss, injury, damage to the BUYER.

4.3 In the event of breach/default by the SELLER in complying and in case the breach/default is not remedied by the SELLER up to period of the notification of the breach/default by the BUYER, the SELLER shall indemnify to the BUYER, to the extent of _______ {(Rs.__________only) being ________3% of the Total Contract Price (including taxes and duties) of _________(Rs. _________only)} of any direct losses or damages suffered by the BUYER due to failure of the SELLER.

4.4 The SELLER shall be fully discharged of its obligations under this bond on meeting its liability as per Para c above which shall be restricted to the limit as provided at Para c above.

4.5 The SELLER shall not be liable for any breach/default arising out of force majeure situation or due to any default, action, inaction or failure on the part of the BUYER. The liability of the SELLER under this bond shall remain and in full force until the fulfilment of the obligations of the SELLER under the said Contract.

4.6 The SELLER hereby expressly, irrevocably, and unreservedly undertake and guarantee that in the event that the beneficiary submits a written demand to SELLER stating that they have not performed according to the warranty obligations for the PRODUCTS as per said Contract, SELLER will pay BUYER on demand and without demur any sum up to maximum amount of _______3% of the Total Contract Price (including taxes and duties). BUYER'S written demand shall be conclusive evidence to SELLER that such repayment is due under the terms of the said contract. SELLER undertakes to effect payment within _____ days from receipt of such written demand.

4.7 The amount of warranty/guarantee shall not be increased beyond 10%. Unless a demand under this warranty/ guarantee is received by SELLER in writing on or before the expiry date (unless this warranty/ guarantee is extended by the SELLER) all rights under this guarantee shall be forfeited and SELLER shall be discharged from the liabilities hereunder. This warranty/guarantee is personal to the BUYER and not assigned to a third party without prior written permission.

5. This Indemnity Bond for Performance-cum-Warranty guarantee shall be governed by Indian Law.

For ________

Signature
Name
Witness
1.
2.

Signature
Name

VERIFIED

Annexure IV to Appendix H
(Refers to Para 8 of this **Appendix**)

FORMAT FOR EXTENSION OF DELIVERY PERIOD/ PERFORMANCE NOTICE

Name of the Procuring Entity ....

Extension of Delivery Period/Performance Notice

To

M/s (name and address of firm)
Sub: Contract No .... dated .... for the supply of ....
Ref: Your letter no .... dated: ....
Dear Sir,

1. You have failed to deliver {the (fill in qty.) of Stores/the entire quantity of Stores} within the contract delivery period [as last extended up to] (fill in date). In your letter under reply you have asked for [further] extension of time for delivery. In view of the circumstances stated in your said letter, the time for delivery is extended from (fill in date) to (fill in date).

2. Please note that notwithstanding the grant of this extension in terms of Clause (fill in clause number) of the subject contract an amount equivalent to __% (______percent) of the delivered price of the delayed goods for each week of delay or part thereof (subject to the ceiling as provided in the aforesaid clause) beyond the original contract delivery date/the last unconditionally re-fixed delivery date (as & if applicable), viz., (fill in date) will be recovered from you as liquidated damages. You may now tender the Stores for inspection [balance of the Stores] in terms of this letter. Stores if any already tendered by you for inspection but not inspected will be now inspected accordingly.

3. You are also required to extend the validity period of the performance guarantee for the subject contract from (fill in present validity date) to (fill in required extended date) within15 (fifteen) days of issue of this amendment letter.

4. The above extension of delivery date will also be subject to the following Denial Clause:-

4.1 That no increases in price on account of any statutory increase in or fresh Imposition of customs duty, GST or on account of any other taxes/duty, including custom duty), leviable in respect of the Stores specified in the said contract which takes place after (insert the original delivery date) shall be admissible on such of the said Stores, as are delivered after the said date; and,

4.2 That notwithstanding any stipulation in the contract for increase in price on any other ground including foreign exchange rate variation, no such increase which takes place after (insert the reckoning date as per DAP 2020) shall be admissible on such of the said Stores as are delivered after the said date.

4.3 But nevertheless, the Buyer shall be entitled to the benefit of any decrease in price on account of reduction in or remission of customs duty, GST or on account of any other Tax or duty or on any other ground as stipulated in the price variation clause or foreign exchange rate variation which takes place after (insert the original delivery date).

5. All other terms and conditions of the contract remain unaltered. This is without any prejudice to Buyer's rights under the terms and conditions of the subject contract.

6. Please intimate your unconditional acceptance of this amendment letter within 10 (ten) days of the issue of this letter failing which the contract will be cancelled at your risk and expense without any further reference to you.

Yours faithfully, (Authorised Officer)
Duly authorised, for and on behalf of
The President of India

Note: Select one option within { } brackets; delete portion within [ ] brackets, if not applicable; fill in ( ) brackets. Brackets and this note are not to be typed.

Substitute following first para instead of first para in format above, for issuing a performance notice.

1. You have failed to deliver {the (fill in qty.) of Stores/the entire quantity of Stores} within the contract delivery period [as last extended up to] (fill in date). In spite of the fact that the time of delivery of the goods stipulated in the contract is deemed to be of the essence of the contract, it appears that (fill in the outstanding quantity) are still outstanding even though the date of delivery has expired. Although not bound to do so, the time for delivery is extended from (fill in date) to (fill in date) and you are requested to note that in the event of your failure to deliver the goods within the delivery period as hereby extended, the contract shall be cancelled for the outstanding goods at your risk and cost.

Annexure V to Appendix H
(Refers to Para 9 & 11 of RFP and para 1.3.7 & 1.3.10 of this Appendix

DELIVERY SCHEDULE AND STAGES OF PAYMENT

1. The terms of payment may vary between each project depending upon a variety of factors such as complexity of equipment/system, delivery period, integration requirements etc. However, some broad guidelines for payments terms are appended in subsequent Paras.

2. **For Delivery in Lots/ Batches**

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
2.1	Signing of Contract	T_0 (0)	10% of the base contract price	APBG of equivalent amount to be submitted	Base price is calculated as total price excluding taxes, AIAMC, manpower, and bandwidth charges for CGWAN.
2.2	On submission of Project report (PR) and Project PERT Chart.	T_0 + 1 month	5% of the base contract price	APBG of equivalent amount to be submitted	Base price is define as above
2.3	**Civil Works**				
2.3.1	Completion of design certification by uptime. Submission of contract copy for civil works. Commencement of civil works.	T_0 + 3 month	10% of the cost of civil works	APBG of equivalent amount to be submitted.	
2.3.2	Completion of excavation for foundation, PCC works in	T0 + 5 months	(aa) 15% of the cost of civil works of DC	APBG of equivalent amount to be submitted.	

VERIFIED

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
	foundation upto plinth beam. Submit application for necessary certification/ clearance for under ground fuel storage tank. (aa) **Data Centre** (ab) **DRDC** (ac) **NLDC**		(ab) 15% of the cost of civil works of DRDC (ac) 15% of the cost of civil works of NLDC	APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.3.3	RCC columns upto roof level including lintel beam and roof casting of first floor. (aa) **DC** (ab) **DRDC** (ac) **NLDC**	T0 + 7 month	(aa) 10% of the cost of civil works of DC (ab) 10% of the cost of civil works of DRDC (ac) 10% of the cost of civil works of NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.3.4	RCC columns upto roof level including lintel beam and roof casting of second floor including roof treatment. (aa) **DC** (ab) **DRDC** (ac). **NLDC**	T0 +10 month	(aa) 10% of the cost of civil works of DC (ab) 10% of the cost of civil works of DRDC (ac) 10% of the cost of civil works of NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch	

VERIFIED

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
2.3.5	Complete internal wiring and plumbing works. Complete plastering (internal and external) and flooring works. (aa) **DC** (ab) **DRDC** (ac) **NLDC**	T0 + 13 month	(aa) 10% of the cost of civil works of DC (ab) 10% of the cost of civil works of DRDC (ac) 10% of the cost of civil works of NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.3.6	Complete joinery works (carpentry). Certification/ clearances for underground fuel storage tank obtained. (aa) DC (ab) DRDC (ac) NLDC	T0 + 14 month	(aa) 5% of the cost of civil works of DC (ab) 5% of the cost of civil works of DRDC (ac) 5% of the cost of civil works of NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.3.7	Completion of finishing works (Painting, distempering etc.) including power backup and cooling of IT and non IT area (aa) DC (ab) DRDC (ac) NLDC	T0 + 15 month	(aa) 5% of the cost of civil works of DC (ab) 5% of the cost of civil works of DRDC (ac) 5% of the cost of civil works of NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	

Sl	**Activity**	**Delivery Timelines (To + Wks)**	**Scheme for Payment**	**Scheme for submission and Return of Advance Payment Bank Guarantees**	**Remarks**
2.3.8	Completion of sanitary and electrical fitting and internal furnishing (creation of office space, common areas, provisioning of furniture's and desktop computers) of non-IT area (aa) DC (ab) DRDC (ac) NLDC	T0 + 16 Month	(aa) 5% of the cost of civil works of DC and 100% cost of the furniture's and desktop computers of non-IT area of DC. (ab) 5% of the cost of civil works of DRDC and 100% cost of the furniture's and desktop computers of non-IT area of DRDC. (ac) 5% of the cost of civil works of DC and 100% cost of the furniture's and desktop computers of non-IT area of NLDC.	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.3.9	Completion of construction certification by uptime. Completion of LEEDS certification for Green Building Norms Final acceptance	T0 + 19 month	(aa) 5% of the cost of civil works of DC (ab) 5% of the cost of civil works of DRDC (ac) 5% of the cost of civil	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
	by ICG (aa) DC (ab) DRDC (ac) NLDC		works of NLDC		
2.4	**Hardware/ Software for DC/ DRDC/ NLDC**				
2.4.1	Delivery of all IT hardware/ software at consignee location and on completion of JRI (aa) DC (ab) DRDC (ac) NLDC	T0 + 12 month	(aa) 60% of the cost of delivered hardware/ software for DC (ab) 60% of the cost of delivered hardware/ software for DRDC (ac) 60% of the cost of delivered hardware/ software for NLDC	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.4.2	Completion of Installations and Commissioning of all hardware/ software (aa) DC (ab) DRDC (ac) NLDC	T0 + 18 month	(aa) 10% of the cost of delivered hardware/ software of DC and 75% of the cost of I&C Charges of DC (ab) 10% of the cost of delivered hardware/ software of DRDC and 75% of the cost of I&C	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
			Charges of DRDC (ac) 10% of the cost of delivered hardware/ software of NLDC and 75% of the cost of I&C Charges of NLDC		
2.5	**Hardware/ Software for Ships**				
2.5.1	Delivery of all IT hardware/ software at consignee location and on completion of JRI	T0 + 06 month	60% of the cost of delivered hardware/ software	APBG of equivalent amount to be submitted.	
2.5.2	Completion of Installations and Commissioning of all hardware/ software	T0 + 06-08 month	10% of the cost of delivered hardware/ software and 75% of the cost of I&C charges		
2.6	**ERP**				
2.6.1	Finalisation of SRS documents for ERP SAFAL. Delivery of ERP licences and development hardware for ERP.	T0 + 06 month	20% of the cost of ERP package excluding hardware cost	APBG of equivalent amount to be submitted.	
2.6.2	Completion of First Pilot implementation demonstration of ERP SAFAL/ MVCR.	T0 + 09 month	15% of the cost of ERP package excluding hardware cost	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	
2.6.3	Second Pilot implementation demonstration of	T0 + 11 Month	15% of the cost of ERP package		

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
	ERP SAFAL/ MVCR.		excluding hardware cost		
2.6.4	Delivery, Installation and Commissioning of ERP hardware	T0 + 06-14 month	70% cost of the ERP hardware and 75% of I&C charges.		
2.6.5	Completion of OEM audit of ERP SAFAL.	T0 + 18 month	10% of the cost of ERP package excluding hardware cost		
2.6.6	Completion of security audit of ERP SAFAL. Submit all licenses and codes in respect of ERP SAFAL	T0 + 20 month	10% of the cost of ERP package excluding hardware cost		
2.7	**Network**				
2.7.1	Placement of orders on Network Service providers.	T0 + 02 month	25% of the network cost except bandwidth and maintenance charges	APBG of equivalent amount to be submitted.	
2.7.2	Completion of site survey and feasibility report of all network nodes.	T0 + 05 month	15% of the network cost except bandwidth and maintenance charges	APBG of equivalent amount to be submitted. APBG is to be returned on pro-rata basis on delivery of each lot batch.	Can be claimed on prorate basis
2.7.3	Establishment of Network Links	T0 + 08-14 month	20% of the network cost except bandwidth and maintenance charges		
2.7.4	Completion of link testing and Commissioning of all network links	T0 + 17-18 month	25% of the network cost except bandwidth and maintenance		

VERIFIED

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
			charges		
2.7.5	One year bandwidth charges	T0 + 18 month onwards	25% on quarterly basis		
2.7.6	One year maintenance charges	T0 + 18 month onwards	25% on quarterly basis		
2.8	**Certifications**				
2.8.1	Completion of Design Certification by uptime	T0 + 03 month	100% lump sum cost of concerned uptime certification charges on submission of relevant certificates		
2.8.2	Construction monitoring and completion of commissioning of data centere certification by uptime.	T0 + 19 month			
2.8.3	Completion of construction readiness and construction certification by uptime.	T0 + 21 month			
2.8.4	Completion of pre-operation and operation certification by uptime.	T0 + 22 month			
2.9	**Final Acceptance and Go-live** Submit all licenses and codes in respect of solutions deployed in DC, DRDC & NLDC. Submit all Audit reports and	T0 + 20-24 month	Balance 10% of the cost of civil works Balance 15% cost of the hardware/ software for DC/DRDC/ NLDC/ Ships/ ERP and balance 10% of I&C charges Balance 15% cost of the		

Sl	Activity	Delivery Timelines (To + Wks)	Scheme for Payment	Scheme for submission and Return of Advance Payment Bank Guarantees	Remarks
	certificates. Signing off project acceptance certificate. Project Commissioning. Final Go-live.		ERP package excluding ERP HW cost.		
2.10	**On-Site Manpower**	TO + 24 months onwards	25% of annual charges on quarterly basis post final go-live		
2.11	**AIAMC Charges**	T0 + 48 months onwards	25% of AIAMC charges on quarterly basis post completion of two years warranty		

Note: ***Reimbursement of taxes and duties will be as per rates and amounts indicated in the commercial bid/contract or as per actuals whichever is lower.***

Appendix J
(Refers to Para 11, 39, 51 and 61.2 of RFP)

EVALUATION CRITERIA AND PRICE BID FORMAT

1. **Evaluation Criteria**. The guidelines for evaluation of Bids will be as follows:-

1.1. The technical proposals forwarded by the Bidders will be evaluated by a Technical Evaluation Committee (TEC). The TEC will examine the extent of variations/ differences, if any, in the technical characteristics/ parameters of the equipment and ERP solution offered by various Bidders with reference to the QRs placed at ***Appendix 'A'*** and prepare a "Compliance Statement" for shortlisting the Bidders.

1.2. The Commercial bids of only those bidders who qualify in the TEC will be opened. The L-1 bidder would be determined by Contract Negotiation Committee (CNC).

2. **Price Bid Format**. The Price Bid Format is given below and Bidders are required to fill this correctly with full details. No column of the Bid format has to be left blank. The clubbing of serials/ sub serials to indicate a consolidated cost is not acceptable. Columns of 'quantity', 'unit cost', 'total cost (including all taxes and duties)', 'GST/ IGST (%) and Custom Duty (%) are to be filled up with '0', 'positive numerical values' or 'Not Applicable' at every row as applicable. If any column is not applicable and intentionally left blank, the reason for the same has to be clearly indicated in the remarks column.

Ser	**Items**	**Qty.**	**Unit Cost**	**Total Cost** **(iii) X (iv)**	**Indicative Rate of Taxes & Duties used to arrive at Total Cost (as applicable)**		**Total Cost (Including all taxes & duties)** **(v) + (vi) +(vii)**	**Remarks**
					GST/ IGST (%)	**Custom Duty (%)**		
(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)
A.	Civil Works	1	Set					
2.1	DC building along with allied facilities and internal furnishings as per requirements specified at Appendix 'A'	1	No					Refer to para 4 – 12 of Appendix 'A'.
2.2	DRDC building along with allied facilities and internal furnishings as	1	No					Refer to para 22 – 33 of Appendix 'A'.

	per requirements specified at Appendix 'A'							
2.3	NLDC along with allied facilities and internal furnishings as per requirements specified at Appendix 'A'	1	No.					Refer to para 40 - 48 of Appendix 'A'.
(B)	Supply of hardware/ software for DC/ DRDC/ NLDC	1	Set					
2.4	Supply of hardware/ software DC as per functional requirements and specifications contained at Appendix 'A' including 02 years warranty	1	Set					Refer to para 52 - 96 of Appendix 'A'.
2.5	Installation, testing, integration and commissioning of hardware/ software for DC	1	set					
2.6	Supply of hardware/ software DRDC as per functional requirements and specifications contained at Appendix 'A' including 02 years warranty	1	No.					Refer to para 52 to 96 of Appendix 'A'.
2.7	Installation, testing, integration and commissioning of hardware/ software DRDC							
2.8	Supply of hardware/ software NLDC as per functional requirements and specifications contained at Appendix 'A' including 02 years warranty	1	Set					Refer to para 52 to 96 of Appendix 'A'.
2.9	Installation, testing, integration and commissioning of hardware/ software NLDC	1	Set					
(C)	Establishment and commissioning of CGWAN	1	Set					

VERIFIED

2.10	Integration, testing & commissioning of MPLS/ VSAT links till DCG commissioning as per requirements specified at Appendix 'A'	210 links	No					Refer to para 100 to 103 of Appendix 'A'.
2.11	One year BW Charges as per requirements specified at Appendix 'A'	1	Yr					Refer to para 103 of Appendix 'A'.
2.12	One year maintenance Charge	1	Yr					
(D)	Supply, development, commissioning SAFAL ERP as per functional requirement and specifications mentioned at Appendix 'A'.	1	Set					Refer to para 107 to 245 of Appendix 'A'.
2.13	Licenses							
2.14	Development							
2.15	Hardware							
2.16	05 years support including ATS (02-year warranty + 03 years AIAMC)							Refer to appendix 'C'.
(E)	Onsite Manpower as specified at Appendix 'A'	1	set					Refer to para 253 and 256 of Appendix 'A'.
(F)	Certifications and Audits as specified at Appendix 'A	1	set					
2.17	Design Certification by uptime							
2.18	Construction monitoring and commissioning of data centere certification by uptime.							
2.19	Construction readiness and construction certification by uptime.							
2.20	Pre-operation and operation certification by uptime.							
(G)	Training as specified at Appendix 'A	1	set					To be imparted free of cost by the bidder
(H)	Documentation as specified at Appendix 'A	1	set					
(J)	Any other							

VERIFIED

	cost (to be specified)							
(K)	**Freight and Transit Insurance** Cost (where applicable).							
(L)	AIAMC							Refer to Appendix 'C'.
(M)	**Total Cost** (Total of Serial A to M)							# This will be used in determining L1 vendor
(N)	Grant Total							

***<u>Note</u>**: (i) **<u>Taxes and Duties</u>**. All Indirect Taxes and Duties will be paid at actuals or as indicated in the Commercial bid by the Bidder, whichever is lower. In case of any change in the tax structure/ rates by BUYER's Government, only incremental/ decremented change will be paid.*

*(ii) Additionally, the bidder would be required to submit a detailed item/ component/ sub-component wise cost of all items indicated in the estimated Bill of Material placed at **Appendix 'Q'** along with completed price bid format. Additional items, if considered necessary, to fulfil the functional requirements/ specifications mentioned at Appendix 'A' may also be listed along with their cost and justification.*

Appendix K
(Refers to Para 56 of RFP)

STANDARD CONDITIONS OF RFP

LAW

1. The present Contract shall be considered and made in accordance to the laws of Republic of India.

ARBITRATION

(For Indian Private Vendors)

2. All disputes or differences arising out of or in connection with the present Contract, including the one connected with the validity of the present Contract or any part thereof, shall be settled by bilateral discussions.

2.1 Any dispute, disagreement of question arising out of or relating to this Contract or relating to construction or performance (except as to any matter the decision or determination whereof is provided for by these conditions), which cannot be settled amicably, shall within sixty (60) days or such longer period as may be mutually agreed upon, from the date on which either party informs the other in writing by a notice that such dispute, disagreement or question exists, will be referred to the Arbitration Tribunal consisting of three arbitrators.

2.2 Within sixty (60) days of the receipt of the said Notice, one arbitrator shall be nominated in writing by SELLER and one arbitrator shall be nominated by BUYER.

2.3 The third arbitrator, shall be nominated by the two arbitrators within ninety (90) days of the receipt of the notice mentioned above, failing which the third arbitrator may be nominated under the provision of Indian Arbitration and Conciliation Act, 1996 or by dispute resolution institutions like Indian Council of Arbitration or ICADR, at the request of either party, but the said nomination would be after consultation with both the parties. The arbitrator nominated under this Clause shall not be regarded nor act as an umpire.

2.4 The Arbitration Tribunal shall have its seat in New Delhi or such other place in India as may be decided by the arbitrator.

2.5 The Arbitration Proceedings shall be conducted in India under the Indian Arbitration and Conciliation Act, 1996 (as amended from time to time) and the award of such Arbitration Tribunal shall be enforceable in Indian Courts only.

2.6 The decision of the majority of the arbitrator(s) shall be final and binding on the parties to this contract.

2.7 Each party shall bear its own cost of preparing and presenting its case. The cost of arbitration including the fees and expenses of the third arbitrator shall be shared equally by the SELLER and the BUYER.

2.8 In the event of a vacancy caused in the office of the arbitrators, the party which nominated such arbitrator, shall be entitled to nominate another in his place and the arbitration proceedings shall continue from the stage they were left by the retiring arbitrator.

2.9 In the event of one of the parties failing to nominate its arbitrator within sixty (60) days as above or if any of the parties does not nominate another arbitrator within sixty (60) days of the place of arbitrator falling vacant, then the other party shall be entitled after due notice of at least thirty (30) days to request dispute resolution institutions in India like Indian Council of Arbitration and ICADR to nominate another arbitrator as above.

2.10 If the place of the third arbitrator falls vacant, his substitute shall be nominated according to the provisions herein above stipulated.

2.11 The parties shall continue to perform their respective obligations under this contract during the pendency of the arbitration proceedings except in so far as such obligations are the subject matter of the said arbitration proceedings.

ARBITRATION

(For Central & State PSEs)

3. In the event of any dispute or difference relating to the interpretation and application of the provisions of the contracts, such dispute or difference shall be referred by either party for Arbitration to the sole Arbitrator in the Department of Public Enterprises to be nominated by the Secretary to the Government of India incharge of the Department of Public Enterprises. The Arbitration and Conciliation Act, 1996 (as amended from time to time) shall not be applicable to arbitration under this clause. The award of the Arbitrator shall be binding upon the parties to the dispute, provided, however, any party aggrieved by such award may make a further reference for setting aside or revision of the award to the Law Secretary, Department of Legal Affairs, Ministry of Law & Justice, Government of India. Upon such reference the dispute shall be decided by the Law Secretary or the Special Secretary/Additional Secretary, when so authorised by the Law Secretary, whose decision shall bind the Parties finally and conclusively. The Parties to the dispute will share equally the cost of arbitration as intimated by the Arbitrator.

ARBITRATION

(For Defence PSUs)

4. In the event of any dispute or difference relating to the interpretation and application of the provisions of the contracts, such dispute or difference shall be referred by either party to the Arbitrator(s) appointed by Defence Secretary. The award of the Arbitrator(s) shall be binding upon the parties to the dispute.

FORCE MAJEURE

5. Should any force majeure circumstances arise, each of the contracting party shall be excused for the non-fulfilment or for the delayed fulfilment of any of its contractual obligations, if the affected party within 30 days of its occurrence informs in a written form the other party.

5.1 Force majeure shall mean fires, floods, natural disasters or other acts such as war, turmoil, strikes, sabotage, explosions, beyond the control of either party.

5.2 Provided the acts of The Government or any state parties of the seller which may affect the discharge of the Seller's obligation under the contract shall not be treated as Force Majeure.

PENALTY FOR USE OF UNDUE INFLUENCE

6. 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 for borne to do any act in relation to the obtaining or execution of the Contract or any other Contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the Contract or any other Contract with the Government. 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 offence 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, 1988 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.

6.1 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.

INTEGRITY PACT

7. Further signing of an 'Integrity Pact' would be considered between government department and the bidder for schemes exceeding **20 Crores**. The Integrity Pact is a binding agreement between the agency and bidders for specific contracts in which the agency promises that it will not accept bribes during the procurement process and bidders promise that they will not offer bribes. Under the IP, the bidders for specific services or contracts agree with the procurement agency or office to carry out the procurement in a specified manner. The essential elements of the IP are as follows:-

7.1 A pact (contract) between the Government of India (Ministry of Defence) (the authority or the "principal") and those companies submitting a tender for this specific activity (the "bidders");

7.2 An undertaking by the principal that its officials will not demand or accept any bribes, gifts, etc., with appropriate disciplinary or criminal sanctions in case of violation;

7.3 A statement by each bidder that it has not paid and will not pay, any bribes;

7.4 An undertaking by each bidder that he shall not pay any amount as gift, reward, fees, commission or consideration to such person, party, firm or institution (including Agents and other as well as family members, etc., of officials), directly or indirectly, in connection with the contract in question. All payments made to the Agent 12 months prior to tender submission would be disclosed at the time of tender submission and thereafter an annual report of payments would be submitted during the procurement process or upon demand of the MoD.

7.5 The explicit acceptance by each bidder that the no-bribery commitment and the disclosure obligation as well as the attendant sanctions remain in force for the winning bidder until the contract has been fully executed;

7.6 Undertakings on behalf of a bidding company will be made "in the name and on behalf of the company's chief executive officer";

7.7 The following set of sanctions shall be enforced for any violation by a bidder of its commitments or undertakings:-

7.7.1 Denial or loss of contract.

7.7.2 Forfeiture of the EMD (Pre-Contract) and Guarantee for Performance-cum- Warranty Bond (after signing of Contract).

7.7.3 Payment to the Buyer of any such amount paid as gift, reward, fees or consideration along with interest at the rate of 2% per annum above LIBOR rate.

7.7.4 Refund of all sums already paid by the Buyer along with interest at the rate of 2% per annum above LIBOR rate.

7.7.5 Recovery of such amount, referred to in (iii) and (iv) above, from other contracts of the Seller with the Government of India.

7.7.6 At the discretion of the Buyer, the Seller shall be liable for action as per extant policy on Putting on Hold, Suspension and Debarment of Entities.

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

7.9 The draft Pre-Contract Integrity Pact is attached as **Annexure to this Appendix.** The vendors are required to sign them and submit separately along with the technical and commercial offers.

7.10 In respect of bids from DPSUs, the concerned DPSU shall enter in to a Pre-Contract Integrity Pact, on the same lines with their sub-vendors individually, in case the estimated value of each sub-contract(s) exceed 20 Crore and such subcontract(s) are required to be entered in to by the DPSU with a view to enable DPSU to discharge the obligations arising out of their bid in question in response to this RFP.

AGENTS

8. The Seller confirms and declares to the Buyer that the Seller System Integrator for requirements referred to in this contract. The Seller confirms that he has not engaged any person, party, firm or institution as an Agent including his Agents already intimated to MoD; to, influence, manipulate or in any way to recommend to any functionaries of the Government of India, whether officially or unofficially, to the award of the contract to the Seller, or to indulge in corrupt and unethical practices. The Seller has neither paid, promised nor has the intention to pay to any person, party, firm or institution in respect of any such intervention or manipulation. 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 Seller has engaged any such person, party, firm or institution and paid, promised or has intention 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 for any or all of the following actions:-

8.1 To pay to the Buyer any such amount paid as gift, reward, fees or consideration along with interest at the rate of 2% per annum above LIBOR rate.

8.2 The Buyer will also have a right to put on hold or cancel the Contract either wholly or in part, without any entitlement or compensation to the Seller who shall in such 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.

8.3 The Buyer will also have the right to recover any such amount referred in 8.1 and 8.2 above from other contracts of the Seller with the Government of India.

8.4 At the discretion of the Buyer, the Seller shall be liable for action as per extant policy on Putting on Hold, Suspension and Debarment of Entities.

9. 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 and clauses relating to Penalty for Use of Undue Influence, the SELLER, on demand of the BUYER shall provide necessary information/inspection of the relevant financial documents/ information, including a copy of the contract(s) and details of payment terms between the vendors and Agents engaged by him.

Annexure to Appendix K
(Refers to Para 20 of RFP and para 7.9 of this Appendix)

PRE-CONTRACT INTEGRITY PACT

General

1. Whereas the PRESIDENT OF INDIA, represented by Joint Secretary & Acquisition Manager (Maritime & Systems)/ Major General & equivalent, Coast Guard, Ministry of Defence, Government of India, hereinafter referred to as the Buyer and the first party, proposes to execute the Digital Coast Guard project, hereinafter referred to as Defence Stores and M/s represented by,Chief Executive Officer (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignees), hereinafter referred to as the Bidder/ Seller and the second party, is willing to offer/ has offered the Defence stores.

2. Whereas the Bidder is a private company/ public company/ partnership/ constituted in accordance with the relevant law in the matter and the Buyer is a Ministry of the Government of India performing its functions on behalf of the President of India.

Objectives

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

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

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

Commitments of the Buyer

4. The Buyer commits itself to the following:-

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

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

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

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

Commitments of Bidders

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

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

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

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

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

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

6.6 The bidder would not enter into conditional contract with any Agents, brokers or any other intermediaries wherein payment is made or penalty is levied, directly or indirectly, on success or failure of the award of the contract. The bidder while presenting the bid, shall disclose any payments he has made during the 12 months prior to tender submission or is committed to or intends to make to officials of the buyer or their family members, Agents, brokers or any other intermediaries in connection with the contract and the details of such services agreed upon for such payments. Within the validity of PCIP, bidder shall disclose to MoD any payments made or has the intention to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution as an annual report during the procurement process.

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

6.8 The Bidder commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts. Complaint will be processed as per **Guidelines for Handling of Complaints** in vogue. In case the complaint is found to be vexatious, frivolous or malicious in nature, it would be construed as a violation of Integrity Pact.

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

7. Previous Transgression

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

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

8. **Earnest Money Deposit**

8.1 Every bidder, while submitting commercial bid, shall submit Bid Security in the form of earnest Money Deposit (EMD, in case where applicable (as provided in clause 8 herein).

8.2 To safeguard against a bidder(s) withdrawing or altering its bid during the bid validity period, Bid security (also known as EMD) is to be obtained from all bidders except for cases upto Rs. 100 croes (i.e. all cases upto Rs. 100 crores of AoN will be exempted from payment of EMD) as follows:-

EMD TABLE

Estimated Cost of Procurement Scheme (Crore)		**EMD Amount**
Above (Not including)	**To (Including)**	
-	100	Nil
100	150	30 Lakh
150	300	70 Lakh
300	1000	2 Crore
1000	2000	5 Crore
2000	3000	10 Crore
3000	5000	15 Crore
5000	-	25 Crore

8.3 EMD is not required from Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase organisation or the concerned Ministry or Department or Startups as recognised by Department of Industrial Policy & Promotion (DIPP), in accordance with the Ministry of Finance office memorandum bearing No.F.20/2/2014-PPD (Pt.) dated July 25, 2017 (as amended from time to time).

8.4 DPSUs are not required to submit EMD when nominated as ab-initio single vendor. DPSUs will submit all BGs and EMD as applicable while participating in multi-vendor cases with private vendors.

8.5 Format of EMD. The Bid Security may be accepted in the following forms, safeguarding the Buyer's interest in all respect:-

8.5.1. Bank Guarantee from any Indian Public or Private Scheduled Commercial Bank notified by RBI or first-class banks of international repute. The format of the Bank Guarantee for Bid Security is provided at Annexure-1 to Appendix O.

8.5.2. Insurance Surety Bond - The format and guidelines pertaining to the same shall be issued/ notified by the Ministry of Defence.

8.5.3. Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque shall be payable in an acceptable form. The Beneficiary Bank Details for furnishing the same are as follows:-

(IFSC Code - SBIN0000691)
State Bank of India New Delhi Main Branch
C Block, 11 Parliament Street
New Delhi, Pin: 110001

8.6 **Validity of EMD**. The EMD will be valid for eighteen months or till signing of contract, whichever is later. The EMD shall be extended from time to time as required by the Buyer and agreed by the Bidder. No interest shall be payable by the Buyer to the Bidder(s) on the EMD for the period of its currency. For unsuccessful bidders EMD will be returned on declaration of successful bidder(s).

8.7 **Instances of Forfeiture of EMD**.

8.7.1. If the Bidder withdraws or amends, impairs or derogates from the Bid in any respect within the period of validity of this tender.

8.7.2. If the Bidder having been notified of the acceptance of his tender by the Buyer during the period of its validity.

8.7.2.1. If the Bidder fails to furnish the Performance Security for the due performance of the contract.

8.7.2.2. Fails or refuses to accept/ execute the contract.

8.7.3 In case of violation of Pre-Contract Integrity Pact, EMD will be forfeited besides other legal penalties as may be decided by the Ministry of Defence.

9. **Company Code of Conduct**

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

10. Sanctions for Violation

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

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

10.1.2 EMD for pre contract period/Performance-cum-Warranty Bond post signing of contract shall stand forfeited either fully or partially, as decided by the Buyer and the Buyer shall not be required to assign any reason therefore.

10.1.3 To immediately cancel the contract, if already signed, without any compensation to the Bidder.

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

10.1.5 To encash the advance bank guarantee and Performance-cum-Warranty Bond if furnished by the Bidder, in order to recover the payments, already made by the Buyer, along with interest.

10.1.6 To cancel all or any other Contracts with the Bidder.

10.1.7 To Put on Hold or Suspend or Debar the bidder as per the extant policy.

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

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

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

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

11. **Fall Clause**

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

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

12. **Independent Monitors**

12.1 The Buyer has appointed Independent Monitors for this Pact in consultation with the Central Vigilance Commission. The names and addresses of nominated Independent Monitors (at the time of issue of RFP) are as follows (however the vendor must refer to the MoD website at www.mod.nic.in to check for changes to these details):-
(*Names & addresses of Independent Monitors holding office on date of issue of RFP to be included)*

12.2 All communications to Independent Monitors will be copied to Director (Vigilance). The Designation and Contact details of Director (Vigilance) are as follows:-

Director (Vigilance)
Ministry of Defence
Room No. 340
B Wing Sena Bhawan
New Delhi – 110 011
Tel No. 011-23012304

12.3 After the Integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the Independent Monitors, if required by them.

12.4 The Bidder(s), if they deem it necessary, may furnish any information as relevant to their bid to the Independent Monitors.

12.5 If any complaint with regard to violation of the IP is received by the buyer in a procurement case, the buyer shall refer the complaint to the Independent Monitors for their comments/ enquiry.

12.6 If the Independent Monitors need to peruse the relevant records of the Buyer in connection with the complaint sent to them by the Buyer, the Buyer shall make arrangement for such perusal of records by the Independent Monitors.

12.7 The report of enquiry, if any, made by the Independent Monitors shall be submitted to the head of the Acquisition Wing of the Ministry of Defence, Government of India for a final and appropriate decision in the matter keeping in view the provision of this Pact.

13. **Examination of Books of Accounts**. In case of any allegation of violation of any provisions of this Integrity Pact or payment of commission, the Buyer or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide

necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

14. **Law and Place of Jurisdiction**

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the Buyer i.e. New Delhi.

15. **Other Legal Actions**

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

16. **Validity**

16.1 The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the Buyer and the Bidder/Seller, whichever is later.

16.2 Should one or several provisions of this Pact turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

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

BUYER

MINISTRY OF DEFENCE GOVERNMENT OF INDIA	CHIEF EXECUTIVE OFFICER
Witness	Witness
1. _______	1. __________
2. _______	2. ___________

BIDDER

*VERIFIED*

(Refers to Para 8.1 of Pre-Contract Integrity Pact)

EMD BANK GUARANTEE FORMAT

Whereas …………………………………… (hereinafter called the "Bidder") has submitted their offer dated…………………………………for the supply of …………………………………… (hereinafter called the "Bid") against the Buyer's Request for proposal No. …………………………………… KNOW ALL MEN by these presents that WE …………………of ………………………………………. having our registered office at ……………………………………. are bound unto …………………. (hereinafter called the "Buyer") in the sum of ……….. ……………………………………………………for which payment will and truly to be made to the said Buyer, the Bank binds itself, its successors and assigns by these presents.

Sealed with the Common Seal of the said Bank this………….. day of ……………20……
The conditions of obligations are:-

(1) If the Bidder withdraws or amends, impairs or derogates from the Bid in any respect within the period of validity of this tender.

(2) If the Bidder having been notified of the acceptance of his tender by the Buyer during the period of its validity.

(a) If the Bidder fails to furnish the Performance Security for the due performance of the contract.

(b) Fails or refuses to accept/ execute the contract.

(3) If the bidder violates Pre-Contract Integrity Pact.

We undertake to pay the Buyer up to the above amount upon receipt of its first written demand, without the Buyer having to substantiate its demand, provided that in its demand the Buyer will note that the amount claimed by it is due to it owing to the occurrence of above mentioned conditions, specifying the occurred condition or conditions.

This guarantee will remain in force upto and including 45 days after the period of 18 months/ contract signing whichever is later and any demand in respect thereof should reach the Bank not later than the above date.
…………………………….

(Signature of the authorized officer of the Bank)
Name and designation of the officer Seal, name & address of the Bank and address of the Branch

VERIFIED

Appendix L
(Refers to Para 57 of RFP)

OPTION CLAUSE

(No blanks to be left)

In case of Indian Bidders. The BUYER shall have the right to place separate order on the SELLER on or before ______________ (_________ year from the date of this Contract) for the main equipment, spares, facilities or services as per the cost, terms and conditions set out in this Contract up to a maximum of 50% quantity and during the original period of Contract provided there is no downward trend in prices. The price of the system, spares etc shall remain same till _________________________ year from the effective date of the Contract. Price Variation Clause, FERV etc, if applicable and included in the original Contract, will also be applicable for Option Clause Contract. For arriving at prices payable, the Price Variation will be applied on the Base Contract price of the original Contact with the month and year of Effective date of Contract as Base Level Indices.

Appendix M
(Refers to Para 4 of RFP)

NON DISCLOSURE AGREEMENT

This Non-Disclosure Agreement is entered into by and between SHQ/MoD (Disclosing Party) and _______________ located at ___________ (Receiving Party) for the purpose of preventing the unauthorized disclosure of confidential information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of the RFP for procurement of (name of the Project).

1. For purpose of this Agreement, "Confidential Information" shall include all information or material in which Disclosing party is engaged. If confidential information is in written form, the Disclosing party shall label or stamp the materials with the word "Confidential" or some similar warning. If confidential information is transmitted orally, the Disclosing Party shall promptly provide a written communication indicating that such oral communication constituted confidential information.

2. Receiving party shall hold and maintain the confidential information in strictest confidence for the sole and exclusive benefit of the Disclosing party. Receiving party shall carefully restrict exercise to confidential information to employees, contractors and third parties as is reasonably required and shall require those persons to sign Non Disclosure restriction at least as protective as those in this Agreement. Receiving party shall not, without prior written approval of Disclosing party, use, publish, copy, or otherwise disclose to others, or permit the use by others or to the detriment of Disclosing party, any confidential information. Receiving party shall return to the Disclosing party any and all record, notes and other written, printed or tangible materials in its possession pertaining to confidential information immediately if Disclosing party requests it in writing.

3. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.

4. If any provision of this Agreement is held to be invalid or unenforceable by court of law, the remainder of this Agreement shall be interpreted so as best to effect the intent of the parties.

5. This agreement expresses the complete understating of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations and understandings. This Agreement shall not be amended except with the written consent of both the parties.

6. That in case of violation of any clause of this Agreement, the Disclosing party is at liberty to terminate the services of receiving party without assigning any reason and shall also be liable to proceeded against in a Court of Law.

7. This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such parties. Each party has signed this Agreement through its authorised representatives.

Disclosing Party

_______________(Signature
_______________(Typed or Printed name)
Date ___________

Received Party

_______________(Signature
_______________(Typed or Printed name)
Date ___________

Appendix N
(Refers to Para 6 of RFP)

CRITERIA FOR VENDOR SELECTION/ PREQUALIFICATION PRE-QUALIFICATION OF BIDS FOR EVALUATION BY TEC FOR INCLUSION IN RFP REQUIREMENTS

1. **Pre-Qualification Criteria**. Bids received from the prospective bidders would be subjected to multiple levels of evaluation. Technical proposals and Commercial bids are required to be submitted in separate sealed envelopes. Upon opening of the bids, the technical bids would be scrutinized by Technical Evaluation Committee for their compliance to the following mandatory pre-qualification criteria:-

Sl.	Parameter	Pre-qualification Criteria	Supporting Documents
1	**Financial**		
(a)	Credit Rating	Long term credit rating of CCR-BBB or better and SME-04 or better as on 31st March of the previous financial year.	
(b)	Average Annual Turn Over	Min Avg Annual Turnover for last 03 financial years, ending 31st March of the previous financial year, should not be less than 100 Cr.	Certificate from CA firm/ P&L statement and Balance sheet approved by the auditor
(c)	Net worth	Net worth of entities, ending 31st march of the previous financial year, should not be less than 31 Cr.	
(d)	Insolvency	The entity should not be under insolvency resolution as per IBC at any stage of procurement process from the issuing of RFP to the signing of contract.	Self-declaration from the bidder in company letter head, signed by authorized signatory.
2	**Technical**		
(a)	Nature of Business	System Integrator of ICT/ Data centres/ Networking of similar nature projects (read with Para 5 & 6 below) and not a trading company, except in cases where OEM participates only through its authorised Vendors.	
(b)	Experience in related field	Min 02 Yrs. experience in System Integration & turnkey projects of similar nature (read with Para 5 & 6 below). If not, then cumulative experience of at least 03 years in system integration, designing & commissioning of data centers /	

		networking. (In case SHQ feels that for particular equipment a lesser experience could be accepted, then the same should be specifically approved by the RFP approving authority before including the same in the RFP).	
(c)	(i) Integration Experience (ii)Turnkey Projects Experience	(i) Experience of not less than one project in integration of similar ICT projects (read with Para 5 & 6 below). (ii) Turnkey Projects - Experience of successful completion of one similar project as defined in para 5 to 6 below within last 05 Years with value of at least 125 Cr. or currently executing a contract of similar nature with value of at least 185 Cr.	Self-certification/ Work order/ relevant completion documents signed by authorized signatory.
(d)	Quality Control	The bidder, in case of single entity or concerned partners in case of Consortiums/ JV should possess below mentioned certifications which are required to be valid at least 18 months from the date of bid submission. In case the validity is due to expire during the intervening period, an undertaking is to be given by the bidder that such certification would be renewed prior expiry:- • CMMi Level-5 • ISO 9001:2008/ ISO 9001:2015 for Quality Management System.. • ISO/IEC 20000: 2011 for IT Service Management.. • ISO 27001:2013 for Information Security Management System • Compliance with IEEE/ ITU standards depending upon nature/ type of project or solution required	Valid copy of certificate.

(e)	Data Centre	Bidder must have established minimum one uptime institute certified Tier – III Data Centre in last five years.	Self- certification/ Work order/ relevant completion documents signed by authorized signatory of the bidder.
(f)		Bidder must have established minimum 55 kW Data Centre Data Centre in last five years.	
(g)	ERP	Bidder must have implemented ERP solution for minimum 4000 ERP licenses.	(i) Self-certified relevant completion documents signed by authorized signatory of OEM/ Bidder (ii) Work order/ relevant completion documents indicating offline capability of the product signed by authorized signatory of the bidder.
(h)		ERP product being offered as part of the solution should have at least one proven deployment in last 05 years.	
(j)		Offered ERP product must have the capabilities of offline deployment.	
(k)	Network	Bidder must have established WAN network connecting minimum 50 sites.	Self-certified relevant ompletion documents signed by authorized signatory of OEM/ Bidder
(l)			
(m)		Bidder must have established minimum one MPLS or VSAT network.	
3	**Others**		
(a)	Industrial License	Posses or be in the process of acquiring a license, if the execution of similar project requires license as per DIPP licensing policy.	
(b)	Registration	The bidder must be incorporated and registered in India under the Indian Companies Act 1956/ LLP Act 2008/ Partnership Act 1932 and Companies Act 2013 should have been operating for min 02 Years. Min no. of years not applicable for JVs constituted specifically for this project.	Certificate of Incorporation/ Copy of Registration Certificate (s)
(c)	Wilful Defaulters	The bidder's Promoters and/ or Directors should not be declared as wilful defaulters in connection with any previous/ ongoing/ prospective contracts concluded/ proposed to be concluded with MoD/ SHQs/ any other	A self-declaration duly certified by a practicing company law expert is to be enclosed.

		Ministries/ Government organisations (as defined in Guidelines for Penalties in Business Dealings with Entities issued vide Ministry of Defence, D(Vigilance) MoD ID No 31013/I/2006- D(Vig) Vol II dated 21 Nov 2016).	
(d)	Blacklisted firm	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

2. The Digital Coast Guard project is complex and technology intensive project which encompasses integration of disparate but interlinked verticals like Data Centre, Networking and ERP development. Successful implementation of the project would therefore entail a detailed evaluation of the bids to ascertain the vendor capability and viability of the bids to meet the project requirements. The acceptance criteria linked to various stages of the project deliveries is also considered essential to ensure compliance of the delivered products/ solutions to the laid down technical specifications and functional requirements. It is therefore felt prudent that a comprehensive evaluation and acceptance criteria is defined with granularity and objectivity.

3. This Appendix lays down the important definitions and criteria for evaluation of the bids.

DEFINITIONS

4. **Bidder**. The term Bidder whenever used in context of this chapter would mean an Indian Vendor as defined at para 20 of Chapter-I of DAP-2020 further qualified by para 2(a) of Annexure-IV to Appendix-A to Chapter-II of DAP-2020.

5. **Similar Projects.** For the purpose of this project, a similar project, wherever referred to in subsequent parts would imply a project, which encompasses all elements envisaged as part of the DCG project, i.e. it should have an element of data Centre/ disaster recovery data Centre implementation, a network implementation, and ERP based solution. However, if a bidder as a single entity may not have executed a single project encompassing all components, at least one of the partner firms in the partnership, JV or the consortium bidding for the project must have undertaken at least one project encompassing one of the components of the DCG project. In case of a consortium, JV or a partnership, the lead bidder must mandatorily have by itself implemented or implementing an ERP intensive project.

6. Further, following criteria will apply for qualifying the project or it's elements to be considered as a similar project:-

(a) Established Data Centre of at least 55 KW capacity and a Disaster Recovery Data Centre of at least half the capacity of the Data Centre.

(b) Undertaken a MPLS/ VSAT network with minimum 50 nodes.

(c) Implementation of proven ERP solution for minimum 4000 ERP licenses consisting at least one module of logistics, finance or HR.

7. To be considered as a similar project, the value of the project, if already implemented should not be less than 125 Crores. Value of the project still under implementation should be not less than 185 Crores.

8. **Indigenous Content**. For the purpose of this Chapter, the term 'Indigenous Content', wherever used would have the same meaning as defined at para 21 of Chapter-I of DAP 2020 and further qualifies by the provisions of Appendix 'B' to Chapter-I of DAP 2020.

Appendix O
(Refers to Para 58 of RFP)

DOCUMENTS TO BE SUBMITTED BY THE BIDDER ALONG WITH THEIR TECHNO-COMMERCIAL PROPOSALS

The list of documents which needs to be mandatorily submitted by the Bidders as part of Technical Proposal are placed below. Non-submission of the documents may result in disqualification of the Bidder from the bidding process.

Sl.	Reference	Document Description
1.	Para 5.1 of part I of RFP	Declaration by Bidder : Debarment of vendors
2.	Para 17 of RFP	Declaration by Bidder: Government Regulation
3.	Para 18 of RFP	Declaration by Bidder: Obligations Relevant to Transfer of Conventional Arms
4.	Para 19 of RFP	Declaration by Bidder : Patent Rights
5.	Para 21 of RFP	Declaration by Bidder : Fall Clause
6.	Para 28 of RFP	Technical document covering performance parameters.
7	Appendix B	Compliance Table
8	Appendix C	Warranty Clause
9.	Appendix E	CERTIFICATE: Malicious Code
10.	Annexure II to Appendix F	Technical Literature
11.	Annexure III to Appendix F	Training Aggregates
12.	Appendix J	Price Bid
13.	Annexure to Appendix K	Pre-Contract Integrity Pact
14.	Annexure to Appendix K	EMD

VERIFIED

Appendix 'P'
(Refers to Para 19 of RFP)

SOFTWARE ARTEFACTS AND ASSOSIATED IPR

Sl.	**Artefact**	**Associated IPR**	**Remarks**
1.	System Design	System Patent	System in entirety
2.	Functional features	Methods Patent	No & listing of functions performed by software
3.	External appearance	Registration of design	GUI menus
4.	Input domain	Registration of design, Patent	Data type, format, source
5.	Processing Algorithm	Method Patent	Algorithms
6.	Compilation script	Copyright	Code specific to OS and compiler
7.	Source Code	Copyright	Code in a programming language
8.	Libraries/ DLLs / Executables	Copyright	The artefact sharing for reuse
9.	Logos/ Images/ Audio files	Copyright	All audio files, images developed for buyer

VERIFIED

Appendix 'Q'
{Refers to note (ii) at Para 2 of Appendix J}

BILL OF MATERIAL

DETAILED BILL OF MATERIAL - DATA CENTRE

Sl.	Generic Description (DC)	CID	Qty.	License Metric
	(A) SUPPLIES - SOFTWARE/ HARDWARE (ONE-TIME) (DC)			
CLOUD				
1	Cloud Management Platform	C01 C02	68	Socket
2	Network and Security Virtualisation	C03	68	Socket
3	Container Management Platform	C04	3	Server
4	Windows Server 2019 Data Centre	C05	3	Server
5	Linux Ent. Server (Socket pair)	C06	8	Server
SERVER & STORAGE				
6	Blade Chassis	C07	4	No.
7	Blade Servers	C07	34	No.
8	Rack Server	C08	5	No.
9	Block & File Storage (Intranet)	C09	1	No.
10	Block & File Storage (Internet)	C10	1	No.
11	Secondary Storage, Webscale, SMB/NFS/S3	C11	1	No.
12	Tape Library	C12	2	No.
13	Back up Appliance	C13	1	No.
NETWORK				
14	Spine Switch	C14	4	No.
15	Leaf - Border/Services/Storage/ OOB Core	C15	4	No.
16	Leaf - Data/Compute	C15	14	No.
17	OOB Management Switch/ WAN Switch	C16	8	No.
18	Core Router	C17	4	No.
19	Virtual Server LB (HA) + WAF+ GSLB	C18	2	Set
20	SDWAN Solution & DC Edge	C19	1	Set
21	SAN Switch	C20	4	No.
22	Passive Cabling	C21	1	Set

SOFTWARE

Sl.	Generic Description (DC)	CID	Qty.	License Metric
23	EMS Suite	C22	1	Set
24	DR Automation	C23	8	Set
25	Back up software	C24	2	Set
SECURITY				
26	SIEM & SOAR	C25	2	Set
27	NGFW Appliance	C26	4	No.
28	Network Detection and packet tracking	C27	2	No.
29	IDAM, SSO	C28	2	Set
30	PAM	C29	2	User Pack
31	End Point Protection, End Point Detection & APT(1+1)	C30	2	Set
32	AAA (in HA)	C31	2	Set
33	PKI Solution	C32	1	Set
34	IT Operation & maintenance services	C33	1	Set
35	Non - IT Operation & maintenance services	C34	1	Set
36	SOC Services	C35	1	Set
SERVICES - AMC/ MANPOWER SUPPORT FOR 05 YRS (ONE-TIME/ RECURRING)(DC)				
Man power, IT Infra & Cloud				
37	Cloud automation, L2, OEM provided	C35	1	No.
38	Virtualisation support, L2	C35	1	No.
39	Network Engineer for NOC, L2, 24x7	C35	1	Set
40	ITOM, ITSM & APM Support, L2	C32	1	No.
41	Server, Storage, Backup, 24x7	C35	1	Set
42	Linux Administrator, L2	C35	1	No.
Manpower, SOC (C37.2)				
	Security Analyst, L2	C34	2	Set
Manpower, Non-ICT				
43	Data Centre Facility cooling, power & floor management, L1, 24x7	C33	1	No.
44	Data Centre Facility cooling, power & floor management, L2	C33	1	No.
45	DCIM, IBMS Support, L2, 24x7	C33	1	No.
46	Fire Prevention & Protection Officer, L2	C33	1	No.
47	Service Desk Support Engineer, 24x7	C33	1	No.
48	Support for L2, L3 offsite manpower, Facility Management	C33	5	Yrs

VERIFIED

DETAILED BILL OF MATERIAL - DISASTER RECOVERY DATA CENTRE

Sl.	Generic Description (DR)	CID	Qty.	License Metric
	(A) SUPPLIES - SOFTWARE/ HARDWARE (ONETIME) (DR)			
CLOUD				
1	Cloud Management Platform	C01 C02	40	Socket
2	Network and Security Virtualisation	C03	40	Socket
3	Container Management Platform	C04	3	Server
4	Windows Server 2019 Data Centre	C05	2	Server
5	Linux Ent. Server (Socket pair)	C06	5	Server
SERVER & STORAGE				
6	Blade Chassis	C07	2	No.
7	Blade Servers	C07	20	No.
8	Rack Server	C08	5	No.
9	Block & File Storage (Intranet)	C09	1	No.
10	Block & File Storage (Internet)	C10	1	No.
11	Secondary Storage, Webscale, SMB/NFS/S3	C11	1	No.
12	Tape Library	C12	2	No.
13	Back up Appliance	C13	1	No.
NETWORK				
14	Spine Switch	C14	2	No.
15	Leaf - Border/ Services/ Storage/ OOB Core	C15	4	No.
16	Leaf - Data/Compute	C15	10	No.
17	OOB Management Switch/ WAN Switch	C16	6	No.
18	Core Router	C17	2	No.
19	Virtual Server LB (HA) + WAF+ GSLB	C18	2	Set
20	SDWAN Solution & DR Edge	C19	1	Set
21	SAN Switch	C20	4	No.
22	Passive Cabling	C21	1	Set
SOFTWARE (As per DR Solution Requirement)				
23	EMS Suite	C22	1	Set
SECURITY (As per DR solution requirement)				
24	SIEM & SOAR	C25	2	Set
25	NGFW Appliance	C26	2	No.
26	Network Detection and Packet Tracking	C27	1	No.
27	IDAM, SSO	C28	2	Set

VERIFIED

Sl.	Generic Description (DR)	CID	Qty.	License Metric
28	PAM	C29	2	User Pack
29	End Point Protection, End Point Detection & APT(1+1)	C30	2	Set
30	AAA	C31	2	Set
31	PKI Solution	C32	1	Set
SERVICES - AMC/ MANPOWER SUPPORT FOR 05 YRS (ONTIME/ RECURRING) (DR)				
	Manpower, IT Infra & Cloud (C37.1)			
32	Virtualisation support, L2	C35	1	No.
33	Network Engineer for NOC, L2, 24x7	C35	1	Set
34	Server, Storage, Backup, 24x7	C35	1	Set
35	Linux Administrator, L2	C35	1	No.
Manpower, SOC (C37.2)				
36	Security Analyst, L2	C34	2	Set
Man	**power, Non-ICT**			
37	Data Centre Facility cooling, power & floor management, L1, 24x7	C33	1	No.
38	Data Centre Facility cooling, power & floor management, L2	C33	1	No.
39	Support for L2, L3 offsite manpower, Facility Management	C33	5	Yrs

DETAILED BILL OF MATERIAL - NEAR LINE DATA CENTRE

Sl.	Generic Description (NLDC)	CID	Qty.	License Metric
	(A) SUPPLIES - SOFTWARE/ HARDWARE (ONE-TIME) (NLDC)			
CLOUD				
1	Cloud Management Platform	C01 C02	10	Socket
2	Network and Security Virtualisation	C03	10	Socket
3	Windows Server 2019 Data Centre	C05	1	Server
4	Linux Ent. Server (Socket pair)	C06	1	Server
SERVER and Storage				
5	Blade Chassis	C07	1	No.
6	Blade Servers	C07	5	No.
7	Block & File Storage (Intranet)	C09	1	No.

NETWORK

Sl.	Generic Description (NLDC)	CID	Qty.	License Metric
8	Spine Switch	C14	1	No.
9	Leaf - Border/Services/Storage/ OOB Core	C15	2	No.
10	Leaf - Data/Compute	C15	2	No.
11	OOB Management Switch/ WAN Switch	C16	4	No.
12	Core Router	C17	1	No.
13	Virtual Server LB (HA) + WAF+ GSLB	C18	1	Set
14	SDWAN Solution & DR Edge	C19	1	Set
15	SAN Switch	C20	2	No.
16	Passive Cabling	C21	1	Set
SECURITY (As per NLDC solution requirement)				
17	NGFW Appliance	C26	2	No.
18	End Point Protection, End Point Detection & APT(1+1)	C30	2	Set

DETAILED BILL OF MATERIAL - REMOTE SITES

SHIP ROBO CLOUD DATA RACKS.

Sl.	Generic Description	CID	Qty.	License Metric
SUPPLIES - SOFTWARE/ HARDWARE/ INSTALLATION/ SUPPORT (ONE-TIME) (ROBO)				
1	Edge Cloud Data Racks with rugged HCA for Ships	C44	88	No.

REMOTE STATIC SITES.

Sl.	Generic Description	CID	Qty.	License Metric
SUPPLIES - SOFTWARE/ HARDWARE/ INSTALLATION/ SUPPORT (ONE-TIME)				
1	Branch SDWAN Edge Devices In HA At Each Site	C19	109	Set

DETAILED BILL OF MATERIAL – ERP

Sl	Items	Qty.
1.	ERP Software (for Heavy Transaction User-250, Light Transaction Users-600, Self Service users - 16,000 & as required. Licenses to include for DevOps and T&D. Warranty for 02 years from final Go	1
2.	Enterprise Database with native replication, security, warranty for 02 years from final go-live. Support for federated database replication across ICG Ships of about 150 Nos.	1
3.	Hardware & related Software (including OS, cloud management platform, Network & Security virtualization, End Point Protection, backup) for DC/ DRDC, OEM warranty for 02 years from installation date. Hardware sizing to include DevOps and T&D environment. (Minimum Hardware sizing mentioned at Para 11.6 below.	1
DESIGN, IMPLEMENTATION & SUPPORT		
4.	Study, design, development & implementation of ERP software including logistics, financial and HR with 02-year warranty post final go-live. Onsite warranty support manpower	1
5.	Audit and Quality Assurance Services from OEM Consultancy Services. OEM should provide design for central and offline ERP module, validate delivery of software for Quality/ Security as per OEM standards. OEM. SI should obtain OEM audit team man-days of minimum of 100 days and provide on-site expert consulting for minimum of 75 man-days. Warranty for 02 year post-final go-live. *1 Man-day is team consisting all skillset	1
6.	Security Audit & VA (Vulnerability Analysis) by CERT-IN empanelled firm of Hardware, ERP Application etc.	1
7.	AIAMC for 03-year post 02 year warranty	2
8.	Training & Documentation	1
OFFLINE ERP MODULE FOR SHIPS, INTERNET		
9.	Study, design, development & implementation of offline ERP software client including logistics, financial and HR. Total Ships are approx. 100 nos. with average Users of 50 Nos. each and internet zone	1
10.	Enterprise Middleware software including Identity Access Management (IAM), warranty for 02 years from final go-live	1
11.	Enterprise software as required. List of software to be provided. Warranty for 02 years from final go-live	1
ONSITE MANPOWER SUPPORT ON AMC		
12.	Functional ERP consultant, L3 level, OEM Certified, 05 years' experience, 03 Nos.	2

13.	Onsite ERP support engineers, L2 level, OEM Certified, 03 years' experience, 06 Nos.	2
14.	Onsite ERP Database Administrator, OEM Certified, 03 years' experience, 02 Nos.	2
15.	Onsite ERP system engineer (02 Nos.), Middleware/ Cloud Automation (02 Nos.) OEM Certified, 03 years' experience	2

Minimum Hardware Sizing.

Sl.	IT Infrastructure Type	SAFAL ERP	CID
1.	All Flash Unified Storage	(a) 40TB available in RAID-6 (b) Qty.- 02 No.	C37
2.	Tape Library	Qty.- 02 No.	C38
3.	Composable IT Infrastructure with SDDC capabilities	(a) Chassis: 02 No. (b) Compute Nodes/ Chassis, 2x20 Cores, 512GB RAM, 2TB SSD in RAID-10: Qty.- 04 Nos. (c) Storage Nodes/ Chassis, 5TB in RAID-10, NL-SAS: Qty.-04 Nos.	C39 C40
4.	Backup Software	02 Socket x 02 Nodes for each of DC & DR	C41
5.	Application Delivery Controller (ADC), Virtual Appliance	(a) 10 Gbps throughput (b) Qty. - 02 Nos. in HA each DC & DR	C42
6.	Rack Server	Qty. 02 Nos.	C43
7.	OEM Qualification, Warranty & Implementation support	Warranty 05 Years from Date of supply	—
8.	Enterprise Database		—

VERIFIED

Appendix R
(Refers to Para 48 of RFP)

PROJECT MANAGEMENT

1. Project timeline should be updated for every versions/ stages as agreed upon during review meetings.

2. **Project Management Server**. Project data sheet should be maintained with MS Project Server for effective monitoring of project progress. Vendor should submit/ upload into ICG project management servers as required by ICG.

3. **Project Team Composition**. The bidder is to engage skilled manpower for the project, who should be available during review meetings as required by ICG. Details of project members alongwith standby members (at least 01 for each) is to be provided prior the first review meeting. Project members should include at least one Senior Project Manager each for DC/ DRDC/ NLDC implementation, Network implementation and ERP project implementation with suitable experience as per industry standards. Additionally, the team should also include a virtualisation expert, cloud expert, security analyst, ERP Functional Consultant, ERP/ Middleware Technical Consultant, Business Analyst, ERP OEM Consultant, and Software Quality Analyst. Project members should not be changed without explicit permission of ICG.

4. **On-site Project Manager**. The bidder shall position an on-site project manager (PM) within one month of signing of the contract. PM shall be responsible for overall project management till go-live, interact with all stakeholders including project development team members and ICG. PM should be PMP Certified, 03 years' experience on project management and should be available till 03 months post-final go-live. PM should also have atleast 03 years of experience in OEM middleware & ERP projects including installation and maintenance.

5. **On-site ERP Functional OEM Consultant**. Bidder shall position onsite ERP Functional Consultant certified/ trained on OEM solution within one month of signing of the contract. Consultant should be well-versed with OEM ALM Agile methodology and should be responsible for management of on-site OEM ALM Software for configuration & customisation related to ERP. Consultant shall be responsible for overall co-ordination validation of Functional aspects of ERP till go-live, interact with all stakeholders including project development team members and ICG. Consultant should have atleast 03 years of experience in relevant ERP project including installation and maintenance. Functional Consultant to be available till final GoLive + minimum 03 months for stabilization.

6. **On-site Business Analyst**. The bidder shall position on-site Business Analyst (BA) duly qualified in Certified Business Analyst Professional (CBAP) Certification/ Equivalent Certification by ERP OEM within one month of signing of the contract. BA shall be responsible for overall co-ordination with Stakeholders, End Users to find & record Business Processes

neutral to any software product/ ERP on SRS/ BA Report on continuous basis. Consultant should have atleast 03 years of experience as BA Analyst. BA to be available till final GoLive + minimum 03 months for stabilization.

7. The Bidder to host in ICG Data Centre and maintain web based detailed project plan including WBS, Resources assigned, Baselines, Critical Path, Stakeholders, Agile sprints, Project Milestones, Activity associated entire software development lifecycle till Go-Live and stabilization. The webbased project plan should be maintained by on-site project manager from the Bidder duly concurred by off-site project technical lead. A dedicated login for the Buyer should be provided from the date of signing of contract.

8. Should provide minimum of 25 Professional User licenses for MS Project Enterprise Server with 25 Professional User. MS Project should be configured with Mobile app to continuously monitor project progress on near real-time/ daily basis. MS Project should be continuously updated by on-site project manager.

9. The bidder shall provide minimum 10 Professional User licenses for CASE (Computer Aided Software Engineering) Server from Visual Paradigm/ Equivalent. CASE Server should be utilised for UML Visual Modelling including BPMN/ ERD, ERP Blueprint Design, Enterprise Architecture, Business Analysis & Design, UI/ UX dynamic wireframes, Conceptual/ Logical Database Design Diagrams, Team Collaboration, Use Case Management, Visual RESTful API Designer, Business Rule Management. CASE Server should be continuously updated by on-site project manager/ off-site Software Architect.

10. The Project Manager should organise meetings, maintain issues on ALM Software to maintain Change Requests, maintain SRS updates, maintain Blue-prints, and responsible to manage software release cycle management.

11. Onsite PM should organise official meetings as required and should submit official Minutes of Meetings (MoM). Only decisions taken on MoM with approval of ICG shall be treated as formal decisions and remaining mode of communications through telephone, emails, meetings without MoM shall be treated as informal and has no binding on ICG.

12. The bidder/ SI should deploy Agile based ERP OEM native Application Lifecycle Management (ALM). ALM to have Task list, Resource scheduling, Resource assignment to Tasks, provide Burn-down Chart, integration to OEM recommended Source Code & Configuration version control Server. ALM to also have native integration into OEM recommended Integrated Development Environment (IDE) for custom development. OEM ALM to be integrated to Unified ICG ALM software based on Atlassian JIRA with licenses as required. Vendor should provide minimum 50 Professional User licenses for JIRA Project Management, Bit Bucket Source Code, Service Desk for ITIL, Confluence for Document Management. JIRA should be deployed in ICG on-campus cloud. OEM ALM and JIRA should be configured with respective Mobile app to continuously monitor issues progress on near real-

time/ daily basis. JIRA should be updated with all project related communications such as Minutes of Meeting, Change Requests, Issues, Features Enhancements, Tickets, As-Is/ To-Be documents. All source code associated with custom development should be maintained in OEM ALM Source Code Server & Bit Bucket Server.

13. The bidder should associate OEM of ERP for necessary consulting services and certification of OEM best practices & ALM methodology compliance which includes detailed Task-Resource mapping, Scheduling, Burn-down chart configurations for real-time monitoring, Source Code & Configuration Management and licensing compliances. OEM Consultant should remain associated till final GoLive of software.

VERIFIED