REQUEST FOR PROPOSAL

FOR

SELECTION OF SYSTEM INTEGRATOR - HARDWARE

FOR

SETTING UP OF DATA CENTRES & INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) EQUIPMENTS

AND

SUPPLY OF COMPUTER HARDWARE & PERIPHERAL EQUIPMENTS, SOFTWARES ETC.

AND

ONSITE COMPREHENSIVE MAINTENANCE OF RELATED COMPONENTS/ITEMS

Authority:
Office of the Registrar General & Census Commissioner, India
Government of India
Ministry of Home Affairs
NDCC-II, A WING, 1ST FLOOR, JAI SINGH ROAD,
NEW Delhi – 110 011

LIST OF ABBREVIATIONS

NDC	National Data Centre
SI-H	System Integrator-Hardware
ICT	Information and Communications Technology
DC	Data Centre
DCC	Data Capture Centre
SITC	Supply, Installation, Testing and Commissioning
CPP	Central Public Procurement
ORGI	Office of the Registrar General, India
DR	Disaster Recovery
SOC	Security Operation Centre
OEM	Original Equipment Manufacturer
EMD	Earnest money deposit
PAO(Census)	Pay and Account Officer (Census)
BOM	Bill of Material
GTV	Gross Total Value
CCA	Controller of Certifying Authorities of India
CA	Certifying Authorities
RCAI	Root Certifying Authority of India
NIT	Notice Inviting Tender
BOQ	Financial Bid
TPEC	Tender Purchase & Evaluation Committee
PBG	Performance Bank Guarantee
TDS	Tax Deduction at Source
SI-H	System Integrator - Hardware
NAC	Network Access Control
SNR	Site Not ready
PoD	Proof of Delivery
HIPS	Host-based Intrusion Prevention System
SIEM	Security Incident & Event Management
SOC	Captive Security Operation Centre
WAF	Web Application Firewall

Table of Contents

SECTION I: ABOUT THE PROJECT 8
a. Background Information 8
b. The scope of the project are as follows: 8
SECTION II: INSTRUCTIONS TO BIDDERS 10
2.1 General Instructions 10
2.2 Obligations of the Systems Integrator Services (SI-H) 15
2.3 General Conditions 16
a. General 16
b. Use & Acquisition of Assets during the term 17
c. Completeness of Response 18
2.4 Pre-Bid Meeting and Clarifications 18
a. Pre-bid Meeting 18
b. Responses to Pre-Bid Queries and Issue of Corrigendum 19
c. Tenure of the Contract 19
2.5. Bid Requirements 19
a. Documents to be submitted along with the Financial Bid (E3): 20
2.6. Preparation of Proposal 23
2.7 Evaluation Process 23
2.8 Tender Evaluation 24
SECTION III: QUALIFICATION & EVALUATION METHODOLOGY 25
3.1 SI-H should either be: 25
3.2 If the OEM as per above is not quoting directly: 25
3.3 The bidder's annual turnover: 25
3.4 Bidder should have the following statutory requirements: 25
3.5 Pre-Qualification for Bidder 26
3.6 Integrity Pact: 27
3.7 Technical Qualification Criteria 28
3.8 Technical Evaluation 29
3.9 Financial Bid Evaluation & Award Criteria 30
3.10 Right to Accept Any Proposal and To Reject Any or All Proposal(s) 31
3.11 Notification of Award 31
3.12 Performance Guarantee 31
3.13 Signing of Contract 31
3.14 Failure to Agree with the Terms and Conditions of the RFP 31
3.15 Project Timelines 32
A. Delivery Process 32
B. Penalty Calculation Process 32
C. Installation Process 33
D. Testing/ Inspection Process 33
E. Onsite Comprehensive Warranty Maintenance 34
SECTION IV: SERVICE LEVEL AGREEMENT 36
4.1 Liabilities and Duties of SI-H 36
4.2 General Conditions 37
4.3 Indemnity 38
4.4 Confidentiality of the Documents and Information 39
4.5 Security of Census Data 39
4.6 Arbitration 40
4.7 Jurisdiction of Courts 41
4.8 Modification of Agreement 41
4.9 Use & Acquisition of Assets during the term 41
4.10 Fraud and Corrupt Practices 42

4.11 Force Majeure....43
4.12 Limitation of Liability....43
4.13 Conflict of Interest....44
4.14 Exit Management....44
4.15 Termination of contract....45
4.16 Application....47
4.17 Standards....47
4.18 Patent Rights....47
4.19 Performance Bank Guarantee and Delivery Schedule....47
4.20 Testing and Acceptance....48
4.21 Spare Parts....48
4.22 Service Facilities....48
4.23 Incidental Services....48
4.24 Training....48
4.25 Proprietary rights....49
4.27 Payment Terms....49
A. Payment of Hardware/software items supplied....49
B. Clarification on Payment....50
C. Penalty....51
4.28 Modification of Tender....52
4.29 Currency of Payment....52
SECTION V: TERMS & CONDITIONS FOR SELECTED BIDDER....53
a. General Conditions....54
b. Miscellaneous....54
c. Applicable Law....54
Annexure – A1: Evaluation Mechanism....55
Annexure – B1: Warranty and Services....57
Annexure – B2: Services to be provided....58
Annexure – B3: Site Not Ready (SNR)....59
Minimum Requirements for Data Centre....60
Design Considerations....60
IT System Design Consideration....60
High Level IT Infrastructure....60
Scalability....61
Availability....62
Interoperability....62
Cyber Security....62
Proposed Architecture....63
DC & DRC Architecture....63
Data Capture Center Architecture....66
Detailed Scope of Work....67
Virtualization Software (Hypervisor) & Manager....67
Network and Security Components....67
Disaster Recovery (DR)....68
Cyber Security Solution....69
DDoS Protection Solution....69
Detection and Mitigation....70
Automated Zero-Day DDoS Attack Protection....70
Integrated Cyber Defense System....70
Next Generation Network Firewall....70
Network Intrusion Prevention System....72
Dedicated Hardware to Fight Attacks....72
Multi-Segment Monitoring and Protection....72
Security Patch Update....72

Application Delivery Controller....72
Web Application Firewall....73
Situational Awareness & Security Analytics....74
DataBase Activity Monitoring (DAM) and Firewall....76
Patch Management Solution....77
Automation....77
Effective Protection Against Vulnerabilities....78
Captive Security Operation Centre (SOC)....79
Security Operation Centre Operation Model....80
SOC Scope of Work:....80
Annexure – C1: List Of Hardware/ Networking Equipment at 18 DCC locations....82
Annexure – C2: Components at 3 Data Centers....83
Annexure – C3: List & Quantity of Software to be installed....84
Annexure – C4: Link Load Balancer for 3 Data Centres....85
Annexure – C5(a): Server with Enclosure Type 1 for 3 Main Data Centres....87
Annexure – C5(b): Server with Enclosure Type 2 for 18 Data Capture Centers....91
Annexure – C6: Workstation....95
Annexure – C7: Mono Laser Printer....97
Annexure – C8(a): MFP – Multifunction Mono Printer....98
Annexure – C8(b): MFP – Multifunction Colour Printer....99
Annexure – C9: SAN Switch for 3 Main Data Centres....100
Annexure – C10: Core Switch Type 1 for 3 Main Data Centres....101
Annexure – C11: Core Switch Type 2 for 18 Data Capture Centres....102
Annexure – C12: Access Switch....103
Annexure – C13(a): Storage of 1PB for 3 Data Centres....104
Annexure – C13(c): Storage for 18 Data Capture Centres....108
Annexure – C14: Backup Software....111
Annexure – C15(a): 200TB Backup Appliance for Data Centre, NDC, ORGI....113
Annexure – C16: On-line Modular UPS Type 1....115
Annexure – C17: Online Modular UPS Type 2....117
Annexure – C20: Online Modular UPS Type 5....119
Annexure – C21: Web Application Firewall....121
Annexure – C22: Database Activity Monitoring (DAM)....123
Annexure – C23: Patch Management Solution....125
Annexure – C24: Host-based Intrusion Prevention System (for Servers)....127
Annexure – C25: SIEM (Security Incident & Event Management)....128
Annexure – C26: End Point Protection and Remediation....130
Annexure – C27: Data Leak Prevention System....132
Annexure – C28: Smart Rack for DR at Lucknow & Bengaluru Data Centres....134
Annexure – C29: Server Rack 42U....137
Annexure – C30: Application Delivery Controller With Global Load Balancing....138
Annexure – C32: Network Intrusion Prevention Specifications (NIPS)....140
Annexure – C33: Captive Security Operation Centre (SOC)....141
Annexure – C33(a): Incident Response services from Security OEM....141
Annexure – C33(b): Threat Intelligence Feed from Global Security Vendor....143
Annexure – C33(c): Onsite Cyber Security Team (Skilled Manpower)....144
Annexure – C34: Router for 3 Main Data Centres....145
Annexure – C35: Firewall with Virtualization....146
Annexure – C36: Network Access Control (NAC)....147
Annexure – C37: Antivirus for 18 DCC locations....150
Annexure – C38: Situational Awareness & Analytics....151
Annexure – C39: Manufacturer Authorization Format....153
Annexure – C40: Format for Declaration by the Bidder for not being Black-listed....154
Annexure – C41: BOM-HW (For Technical Bid)....155

Annexure - D2: PRICE SCHEDULE 157
Annexure – L: List of Data Centers/Data Capture Centers 160
Annexure – M: Data Centre-wise Numbers of Hardware items for Buy Back 161
Annexure – N: Qualification and Experience of Service/Resident Engineer 162
Annexure – O: STATEMENT OF DEVIATIONS FROM TECHNICAL SPECIFICATIONS 163
Annexure – P: STATEMENT OF DEVIATIONS FROM TENDER TERMS AND CONDITIONS 164
Annexure – Q: SCHEDULE OF DELIVERY 165
Annexure – R: UNDERTAKING BY THE BIDDER 166
Annexure-S: Format for Undertaking by the Bidder/Contractor 168
Annexure-T: IMPORTANT DATES AND ACTIVITIES 170

ORGI

Datasheet

Sl. No.	Item	Description
1	Name of the RFP	Selection of System Integrator-Hardware (SI-H) for Setting up of 3 Data Centers including installation, operation & comprehensive maintenance of Information and Communications Technology (ICT) Equipment's, and Supply, installation and on-site comprehensive maintenance of Computer Hardware, related Peripheral equipment and Software at 18 DCCs and NDC, ORGI under Office of the Registrar General India, Ministry of Home Affairs.
2	Tender Inviting Authority	Joint Director, Office of the Registrar General, India
3	Bid submission	Bids have to be submitted online on the Central Public Procurement Portal (URL: http://eprocure.gov.in).
		Bidders will have to submit EMD in a sealed envelope as per the last date and time of bid submission at JD(HO), 1st floor, A wing, NDCC-II Building, Jai Singh Road, New Delhi – 110001.
4	Method of Selection	Least Cost Basis method
5	Availability of RFP documents	RFP would be available on ORGI website at www.censusindia.gov.in and https://eprocure.gov.in/epublish/app
6	Date of RFP issue	12/09/2019
7	Bid Security/ Earnest Money Deposit (EMD)	INR 2,00,00,000/- (Rupees Two Crore) in the form of DD or Bank Guarantee from a nationalized / scheduled bank in favor of: Pay and Account Officer (Census), MHA, payable at New Delhi
8	Last date for download of RFP	Same as bid submission date
9	Last date for Submission of Pre-Bid Queries	Time: 06:50 PM Date: 15/09/2019
		All pre-bid queries are required to be submitted in spreadsheet format by Bidders to the email id : jslamba.rgi@gov.in with the following subject heading: **"Pre-Bid Queries for SI-H from <Name of OEM/SI-H>"**
10	Pre-Bid Conference Time, Date, & Venue	Time: 3:00 PM Date: 19/09/2019
		Venue: Conference Room, Office of the Registrar General, India, Ground floor, Wing 1, West Block 1, R K Puram, New Delhi 110063
11	Publishing of Responses to pre-bid queries / corrigendum by ORGI	To be intimated later.
		Responses to the pre-bid queries would be published on www.censusindia.gov.in and https://eprocure.gov.in/epublish/app
12	Bid Submission Start Date	12/09/2019
13	Last date and time for Bid/Proposal submission (on or before)	Time: 3:00 PM Date: 30/10/2019
14	Bid Opening Date	Time 3.30 PM Date: 31/10/2019
15	Date for Technical Presentation by Bidders	To be intimated later
16	Date and time for Opening of Commercial Bids.	To be intimated later
17	Language of Bid Submission	Proposals should be submitted in English only
18	Bid Validity	Proposals must remain valid up to 120 (One Hundred Twenty) days from the last date of submission of the Bids.
19	Currency	Currency in which the Bidders shall quote the price and will receive payment is INR only
20	Name and Address for Communication and seeking clarifications	Joint Director (IT), NDC, ORGI, MHA, 8th FLOOR, BLOCk-3, DMRC IT PARK, SHASTRI PARK, DELHI – 110 053

SECTION I: ABOUT THE PROJECT

a. Background Information

The Office of Registrar General of India herein referred to as (ORGI) proposes to undertake data capture and data processing activities for Census of India 2021, at 19 of its sub-offices in India, which includes 3 main Data Centre (DC) and 18 Data Capture Centers (DCCs) (Annexure – L). Under the project, the ORGI intends to select One System Integrator-Hardware (SI-H) to supply, install and maintain Server, Workstation, Storage, Printers, UPS, Network & Security devices/ firmware and establishing of LAN etc.

b. The scope of the project are as follows:

1.1 To setup 3 main Data Centers at Delhi, Bengaluru, Lucknow to host online census applications. Main Data Centers will be connected over to internet and shall be provided by ORGI. These Data Centers will have latest technology using state of art Compute, Storage, Network & Security equipment along with modular UPS. These Data Centers should be properly secured using state of art technology including Next Generation Firewall, DDoS protection, NIPS, Patch Management, HIPS, End point Protection, Web Application Firewall.

1.2 National Data Center (NDC), ORGI at Shastri Park, Delhi will be the main Data Centre, from where other two Data Centres namely Bengaluru and Lucknow will be managed. SOC will also be established at NDC, ORGI at Delhi.

1.3 Supply and Installation of Server, Workstation, Storage, Printers, UPS, Network & Security devices/firmware etc.

1.4 Supply & installation of Operating Systems, other Software and driver software for various components of Systems hardware. All driver software will be arranged by selected SI-H.

1.5 LAN of 18 Data Capture Centers (DCCs) i.e. Chandigarh, Dehradun, Delhi(R.K.Puram), Jaipur, Lucknow, Patna, Guwahati, Kolkata, Ranchi, Bhubaneswar, Raipur, Bhopal, Gandhinagar, Mumbai, Hyderabad, Bengaluru, Thiruvananthapuram and Chennai will not be connected over to internet. These DCCs will be used for Intelligent Character Recognition (ICR) Processing of census paper schedules and have Servers, Storage, Network, Workstations, Printers and UPS. Two DCCs i.e. Bengaluru and Lucknow will be used as DCC as well as Disaster Recovery(DR) Centres also.

1.6 To maintain all of the hardware/software items referred above for a period of 5 years from the date of acceptance of the System by ORGI. The warranty on UPS batteries will be minimum for three years.

1.7 To provide one Resident Service Engineer, for on-site support for 5 years, at all the 19 locations including NDC, Shastri Park and 2 DR sites i.e. Bengaluru and Lucknow from date of installation and acceptance of the hardware/software.

1.8 To provide a team of at least two persons per shift for management, monitoring and operations of Network & Security Services along with Storage and Server management at

each site namely at (i) NDC, Shastri Park, Delhi (ii) Lucknow (iii) Bengaluru, initially for two year from the date of installation and acceptance of the hardware/software which may be extended as per requirement. However, the number of shifts, location and persons may vary depending upon the requirement of ORGI/DCOs. These persons should be **certified engineers from offered OEM.** These persons would be in addition to the resident engineers mentioned at Para 1.7.

1.9 To provide the training to DCC and NDC officials at 19 locations.

1.10 To make all the Data centers/ DCCs operational after installation, interconnection, configuration and integration of hardware and software.

1.11 In order to make system fully integrated up and running, any other components like power cable, patch-cords (Fx, Tx), connectors, PDU, etc should be provided by successful bidder.

1.12 To provide full support in resolving any issue related to hardware installed for capturing the data through mobile / web applications.

1.13 To buy-back the old equipment at all locations (Please refer Annexure-M.

1.14 Setting up of Security Operation Centre (SOC) (Please see **Annexure C33** for details).

1.15 Shifting of Hardware among 3 DC and 18 DCC: Depending upon workload requirements, SI-H will provide assistance in uninstalling, shifting and reinstallation of hardware items supplied by bidder. However Freight, insurance (if required) charges shall be borne by ORGI/DCO. The bidder is expected to install, uninstall any hardware/ software, for above purpose not more than twice during the contract period at No extra charges.

SECTION II: INSTRUCTIONS TO BIDDERS

2.1 General Instructions

1. All interested bidders are requested to register themselves with the portal http://eprocure.gov.in and enroll their digital certificate with the user id for participation in the tender.

2. Bidders are requested to read following conditions in conjunction with various conditions, wherever applicable appearing with this bid invitation for e-Tendering. The conditions mentioned here in under shall supersede and shall prevail over the conditions enumerated elsewhere in the tender document.

Bidders are advised to check the CPPP website https://eprocure.gov.in/eprocure/app at least 3 days prior to the closing date of submission of tender for any corrigendum, addendum, or amendment to the RFP document.

3. How to submit On-line Bids / Offers electronically against e-Tendering?

Vendors / Bidders are advised to read the following instructions for participating in the electronic tenders directly through internet:

i) Late and delayed Bids / Offers after due date / time shall not be permitted in e-Tendering system. No bid can be submitted after the last date and time of submission is over. (However if bidder intends to revise the bid already submitted, they may change / revise the same on or before the last date and time of submission of bid). The system time (IST) that will be displayed on e- tendering web page shall be the time and no other time shall be taken into cognizance.

ii) Bidders are advised in their own interest to ensure that bids are uploaded in e-tendering system well before the closing date and time of bid.

iii) No bid can be modified after the dead line for submission of bids.

iv) No manual bids/offers along with electronic bids/offers shall be permitted.

4. What is a Digital Signature?

This is a unique digital code which can be transmitted electronically and primarily identifies a unique sender. The objective of digital signature is to guarantee that the individual sending the message is who he or she really claims to be just like the written signature. The Controller of Certifying Authorities of India (CCA) has authorized certain trusted Certifying Authorities (CA) who in turn allots on a regular basis Digital Signature Certificates.

5. Documents which are signed digitally are legally valid documents as per Indian IT Act (2000).

6. Why is a Digital Signature required?

In order to bid for ORGI e-tenders all the vendors are required to obtain a legally valid Digital Certificate as per Indian IT Act from the licensed Certifying Authorities (CA) operating under the Root Certifying Authority of India (RCAI), Controller of Certifying Authorities (CCA) of India. The Digital Certificates is issued by CA in the name of a person authorized for filing Bids / Offers on behalf of his Company. A Vendor / Bidder can submit their Bids / Offers on-line only after digitally signing the bid / documents with the above allotted Digital Signatures.

7. Bidders have to procure Digital Signature Certificate (Class 3 or 2 with signing key uses) from any of the certifying Authorities in India.

8. Submission of Documents:

i) Bidders must submit on line offers by the date and time mentioned in the RFP at the website address stated therein.
ii) Each E-Tender will provide access to Commercial as well as Price part of tender. Along with the Commercial part, Bidders can attach the required documents with the bid in line with the Tender.
iii) The successful bid submission can be ascertained once acknowledgement is given by the system through bid submission number after completing all the process and steps.
iv) The bid have to be submitted online only. However, EMD (in original) is to be submitted to Joint Director (HO), 1st floor, A wing, NDCC-2 Building, Jai Singh Road, New Delhi – 110001. The EMD in the form of Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any of the Commercial Banks in favour of "**Pay and Account Officer (Census)**", payable at New Delhi. ORGI shall not be responsible in any way for failure on the part of the bidder to follow the instructions. Physical Bids will not be accepted. All such physical Bids shall be considered as invalid offers and shall be rejected summarily without any consideration..
v) Price Bid shall contain only price as per Schedule of Rates (in form of an excel sheet) without any condition. The lump sum rate along with tax and other components shall be filled up in figures and the total amount shall be automatically calculated and rounded off to the nearest rupee. It is to be noted that the Price Bid shall contain only PRICES and no conditions whatsoever.
vi) The bid shall be uploaded through Digital signatures by someone legally authorized to enter into commitment on behalf of the Bidder. Bidder shall upload among other documents, power of Attorney in favour of the person who is authorized to enter into commitments on behalf of the Bidder.
vii) It is advised that the bidder upload small sized documents (preferably upto 5 MB) at a time to facilitate in easy uploading into e-tendering site. ORGI does not take any responsibility in case of failure of the bidder to upload the documents within specified time of tender submission.

9. Submission and Opening of Bids

i) Bid along with all the copies of documents should be submitted in the electronic form only through ORGI e-tendering system. Before the bid is uploaded, the bid comprising of all attached documents should be digitally signed using digital signatures issued by an acceptable Certifying Authority (CA) in accordance with the Indian IT Act 2000.
ii) The bid shall be opened on-line on the date & time mentioned in the RFP.
iii) The Price Bids of only those bidders shall be considered for electronic opening & evaluation, whose bid is determined to be technically acceptable to ORGI.

10. Last Date for Submission of Bids: Bidders are advised in their own interest to ensure that bids are uploaded in e-Procurement system well before the closing date and time of bid. Vendors / Bidders must use any computer having Windows version 7 or higher of Window operating system and an internet web browser version internet explorer v8.0 or higher recommended.

12. In case of the Two-bid system, only the Technical Bid would be opened on the time and date mentioned above. Date of opening of the Commercial Bid will be intimated after acceptance of the Technical Bids. Commercial Bids of only those firms will be opened, whose Technical Bids are found compliant/suitable after Technical evaluation is done by the ORGI.

13. Clarification regarding contents of the RFP: A prospective bidder who requires clarification regarding the contents of the bidding documents shall notify to the ORGI in writing about the clarifications sought not later than the date mentioned in the schedule prior to the date of opening of the Bids. Copies of the query and clarification by the purchaser will be sent to all prospective bidders who have received the bidding documents.

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

16. Rejection of Bids: Canvassing by the Bidder in any form, unsolicited letter and post-tender correction may invoke summary rejection with forfeited of EMD. Any commercial condition having financial implication in the tender will be rejected.

17. Validity of Bids: The Bids should remain valid for 120 days from the last date of submission of the Bids.

19. The tender shall be submitted in major parts, namely Technical Bid and financial Bid (BOQ).

20. As a part of software requirement for the e-tender, the main features are:
i) The price bid formats are same for global and Indian vendors. Bidders are requested to follow the instructions mentioned in the bid format.

ii) Vendors interested in the tender may submit scanned copy of EMD as stated in document in this e-tender and submit the original EMD physically within the closing time & date as mentioned.

21. In respect of Two-Bid system, bidders are required to furnish clause by clause compliance of specifications bringing out clearly the deviations from specification, if any. The bidders are required to quote only one product against each line item which meets the product specification requirement in the bid document otherwise bid will not be considered for further evaluation and compatible spare parts will not be accepted.

22. It is mandatory for every bidder to fill all the documents as set out in the tender document irrespective of their earlier association with ORGI. Any conditional / incomplete offer or failure to follow above instructions shall lead disqualification even at the time of opening of bids.

23. Variation on government duty and taxes based on turnover of the bidder/company will not be allowed.

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

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

26. Goods and Service Tax (GST):

Pursuant to the notification of GST Act 2017, the rate of GST as applicable to the tendered item should be correctly quoted by the tenderer, duly mentioning the HSN code. The offers will be evaluated based on the GST rate as quoted by each bidder and same will be used for

determining the inter-se ranking. While submitting offer, it shall be the responsibility of the bidder to ensure that they quote correct GST rate and HSN number. Purchaser shall not be responsible for any misclassification of HSN number or incorrect GST rate if quoted by the bidder.

Wherever the successful bidder invoices the Goods at GST rate or HSN number which is different from that incorporated in the purchase order, payment shall be made as per GST rates which is lower of the GST rate incorporated in the purchase order or billed. Vendor is informed that she/he would be required to adjust her/his basic price to the extent required by the higher tax billed as per invoice to match the all inclusive price as mentioned in the purchase order.

Any amendment to GST rate or HSN number in the contract shall be as per the contractual conditions and statutory amendments in the quoted GST rate and HSN number, under SVC.

27. If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price will prevail and the total price will be corrected.

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

29. Penalty for use of Undue influence: The Bidder undertakes that he has not given offered or promised to give, directly or indirectly, any gift, consideration, reward commission, fees, brokerage or indecent to any person in service of the ORGI or otherwise in procuring the Contracts or forbearing to do or for having done of forborne to do any act in relation to the obtaining or execution of the present Contract or any other Contract with the Government of India for showing or forbearing to show favour or disfavour to any person in relation to the present Contract or any other Contract with the Government of India.

Any breach of the aforesaid undertaking by the 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 offers by the Bidder or anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the ORGI to cancel the contract and all or any other contracts with the Bidder and recover from the Bidder the amount of any loss arising from such cancellation.

A decision of the ORGI or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Bidder. Giving or offering of any gift, bribe or inducement or any attempt at any such act on behalf of the Bidder towards any officer/employee of the ORGI or to any other person in a position to influence any officer/employee of the ORGI for showing any favour in relation to this or any other contract, shall render the Bidder to such liability/penalty as the ORGI 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 ORGI.

2.2 Obligations of the Systems Integrator Services (SI-H)

a) While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements.

b) All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by the ORGI on the basis of this RFP.

c) No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract/agreement has been executed by or on behalf of ORGI. Any notification of preferred bidder status by ORGI shall not give rise to any enforceable rights by the Bidder. ORGI may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of ORGI.

d) The SI-H will provide different categories of required nos. of manpower at 18 nos. of DCCs and NDC, ORGI as per the details provided in RFP. However, ORGI/DCO reserves the right to increase/decrease the numbers of manpower at any particular DCC (depending upon the urgency of requirement and work load), anytime during the period of contract. The increase/decrease in requirement may be conveyed to SI-H by an authorised officer of the ORGI/DCO;

e) The Qualification, Job descriptions and responsibilities of Manpower deployed by the SI-H is shown in the Annexure-M;

f) The services rendered by the SI-H under this Agreement shall be under close co-ordination and guidance/instruction of the ORGI/DCO. SI-H shall frame appropriate procedure for taking immediate action as may be advised by ORGI/DCO from time to time;

g) The SI-H shall decide the Modus Operandi to engage the manpower deployed by it for rendering proper and efficient services and to conform to its prescribed standards;

h) The manpower deployed by the SI-H shall not install/use any other unauthorised software etc. (except pre-installed licensed software) and shall not misuse the computer systems of ORGI;

i) If the ORGI/DCO notices that the manpower deployed by SI-H has/have been negligent and careless in rendering the said services, the same shall be communicated immediately to the SI-H. The SI-H will take corrective action immediately, to avoid recurrence of such incidents, which may include providing proper substitutes;

j) If any manpower deployed by the SI-H indulges in theft, misconduct or any illegal/irregular activities, the SI-H will initiate appropriate action against such manpower besides providing suitable substitutes in its place;

k) ORGI/DCO shall be at liberty to object to and require the SI-H to remove any manpower deployed by SI-H, who in the opinion of ORGI/DCO is incompetent or negligent in the proper performance of his duties;

l) The ORGI/DCO shall not be held responsible fully or partly, to any dispute or difference, that may arise between the SI-H and the manpower engaged by it for the said services;

m) At times, in case of exigencies of work, the manpower may be required to work beyond office hours, for which no additional payment will be made by ORGI to the SI-H;
n) The SI-H shall employ only such persons as are qualified and skilled for carrying out the assigned jobs as detailed in Para (d) above. The SI-H shall submit the particulars of all personnel deployed as per format given in Annexure-M along with 2 photographs;
o) Before deployment of manpower, SI-H shall check and verify the antecedents of the manpower deployed on duty. All the manpower deployed under this contract shall be of good character, well-behaved and disciplined. The liability of the conduct & discipline of the deployed manpower shall rest with the SI-H. The SI-H will submit the undertaking as per the format given in Annexure-M about the antecedents, police verification, character, conduct & discipline of the manpower deployed by it;
p) The SI-H shall be responsible for the proper behavior of the manpower deployed and shall exercise proper control over them, and to ensure that their activities shall not in any way be detrimental to the ORGI/DCO. The SI-H shall have to withdraw such manpower with immediate effect, if so desired by the ORGI/DCO or its authorised representative(s);
q) The ORGI/DCO reserve the right to order any manpower of the SI-H to leave its premises, if his/her presence at any time is felt undesirable;
r) The SI-H shall issue Identity Cards on its own name and trading style, to its manpower deployed for rendering the said services, which at ORGI's option, would be subject to verification at any time. The ORGI/DCO may refuse the entry into its premises to any manpower of the SI-H not bearing such identity card;
s) No manpower of the SI-H shall enter into any other area of the ORGI/DCO premises, except to the area of the premises (DCC) where they have been deployed, without the permission of the ORGI/DCO;
t) It is understood between the parties hereto that the SI-H alone shall have the right to take disciplinary action against any manpower engaged/ deployed by it, while no right shall vest in any such manpower to raise any dispute and/or claim whatsoever against the ORGI/DCO. ORGI/DCO shall under no circumstances be deemed or treated as the Employer in respect of manpower engaged/deployed by the SI-H for any purpose, whatsoever, nor would ORGI/DCO be liable for any claim(s) whatsoever, of any such manpower;

2.3 General Conditions

a. General

a) While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements.
b) All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the contract by the ORGI on the basis of this RFP.
c) No commitment of any kind, contractual or otherwise shall exist unless and until a

formal written contract/agreement has been executed by or on behalf of ORGI. Any notification of preferred bidder status by ORGI shall not give rise to any enforceable rights by the Bidder. ORGI may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of ORGI.

d) Bidders are advised to study the Bid Document carefully. Submission of the Bid shall be deemed to have been done after careful study and examination of all instructions, annexures, eligibility, forms, compliance statements, terms and requirement specifications, BOM (Annexure C41 - Bill of Material) formats in the tender document with full understanding of its implications. Bids not complying with all the given clauses in this tender document are liable to be rejected. Failure to furnish all information required by the tender document or submission of a bid not substantially responsive to the tender document in every respect will be at the Bidder's risk and may result in the rejection of the bid.

b. Use & Acquisition of Assets during the term

During the Term of the Agreement, SI-H shall:

i. Take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components, Deliverables used for the project and other facilities leased/owned/operated by SI-H exclusively in terms of the delivery of the services as per the CA (hereinafter the "Assets") in proportion to their use and control of such Assets which will include all upgrades/enhancements and improvements to meet the needs of the project arising from time to time

ii. Term "Assets" also refers to all the hardware / Software / furniture / data / documentations / manuals/ or any other material procured, created or utilized by SI-H or ORGI for implementation of IT Infrastructure solution.

iii. Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) as on the date SI-H takes control of and/or first uses the Assets suitably upgraded subject to the relevant standards as stated in the bid to meet the SLAs mentioned in the contract and during the entire term of the Agreement

iv. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets and which are provided to SI-H will be followed by SI-H and any person who will be responsible for the use of the Asset

v. Take such steps as may be recommended by the manufacturer of the Assets and notified to SI-H or as may in the reasonable opinion of SI-H be necessary to use the Assets in a safe manner

vi. To the extent that the Assets are under the control of SI-H, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them and as per the terms agreed with ORGI

vii. Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law

viii. Use the Assets exclusively for the purpose of providing the Services as defined in the contract

ix. Ensure the integration of the software with hardware to be setup and the current Assets in order to ensure the smooth operations of the entire solution architecture to

provide efficient services to ORGI of this Project in an efficient and speedy manner

x. SI-H shall not use ORGI data to provide services for the benefit of any third party, as a service bureau or in any other manner

xi. Use best efforts to ensure that no lien, mortgage, hypothecation or any other charge is created over the Assets. SI-H agrees that SI-H will inform ORGI immediately if SI-H feels or comes to know that a charge may be / has been created over any Asset(s). In the event a charge is created over any of the Assets which are owned by, ORGI shall have the right to get the charge removed at the risk, cost, expense of SI-H and SI-H shall make good all losses, damages, costs, fees, cess, duties, etc. borne or suffered by ORGI due to creation of such charge and/or in removal of such charge and/or in discharging the obligations for removal of such charge.

c. Completeness of Response

a) Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of the bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.

b) Failure to comply with the requirements of this paragraph may render the Proposal non- compliant and the Proposal may be rejected. Bidders must:

i. Include all documentation specified in this RFP;

ii. Follow the format of this RFP and respond to each element in the order as set out in this RFP;

iii. Comply with all requirements as set out within this RFP.

2.4 Pre-Bid Meeting and Clarifications

a. Pre-bid Meeting

a) ORGI shall hold a pre-bid meeting with prospective bidders on the date, time & venue as mentioned in “Data Sheet”.

b) Entry of maximum three persons per prospective bidder will be permitted in Pre-Bid meeting. Interested bidders are requested to intimate about their participation in Pre-Bid meeting at least two days before Pre-Bid Meeting.

c) The Bidders will have to ensure that their queries for Pre-Bid meeting should reach to Nodal Officer at **email ID: jslamba.rgi@gov.in** on date and time as per “Data Sheet”.

d) The queries should necessarily be submitted in the following format, with the subject mentioning **“Pre-Bid Queries for SI-H from <Name of OEM/SI-H>”**:

S. No.	RFP Document Reference & Page Number	Content of RFP requiring Clarification(s)	Points of clarification
1.			
2.			
3.			

e) ORGI shall not be responsible for ensuring that the bidders’ queries have been received by them. Any requests for clarifications post the indicated date and time may not be entertained by the ORGI.

b. Responses to Pre-Bid Queries and Issue of Corrigendum

a) The Nodal Officer notified by the ORGI will endeavour to provide timely response to all queries. However ORGI makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does ORGI undertake to answer all the queries that have been posed by the bidders.

b) At any time prior to the last date for receipt of bids, ORGI may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by a corrigendum.

c) The Corrigendum (if any) & clarifications to the queries from all bidders will be posted on the ORGI website.

d) Any such corrigendum shall be deemed to be incorporated into this RFP.

e) In order to provide prospective Bidders reasonable time for taking the corrigendum into account, ORGI may, at its discretion, extend the last date for the receipt of Proposals.

c. Tenure of the Contract

The contract would be valid for five years from the date of acceptance of HW/Services by ORGI. In addition, the contract may be extended for successive months, upto a period of 36 months with mutual consent, as per price bid and on same terms and conditions.

2.5. Bid Requirements

1 The Bidder must quote for all Items and Quantities as listed in the in the Price Schedule (Annexure D-2). Offer for part quantity and/or part items shall not be considered and rejected without further reference.

2 Bidders should enclose, along with the Technical Bid of their offers, the full details of equipment/items offered along with list of consumables with their life and price. Full documentation, descriptive literature/leaflets supplementing the description and point out any special feature of their system. All documentation is required to be in English.

3. **Documents to be uploaded along with the Eligibility and Technical Bid (E2):** The Technical Bid should be submitted by the bidder and should not contain any price information regarding the items/services included therein and it shall comprise of all documents in support of the eligibility criteria and the following technical-support documents to be enclosed for all technical annexure:

   i. Original catalogue of the products quoted.

   ii. Necessary detailed technical write up highlighting the features of the sub assemblies of the systems offered.

   iii. Information on planned future upgrades and compatible products along with the anticipated time frame.

   iv. List of important installation sites having similar equipment as quoted in the technical bid.

   v. List of service centers located across India along with address and contact details.

vi. For all the quoted items, make and model should be mentioned in the technical bid along with complete details. The items quoted should be new, good quality and with latest hardware/software version. The beta version and product which are not launched before three months of the bid date should not be quoted.

vii. Un-priced Bill of Material along with part numbers, make and model for main items quoted for each Server, Client, Storage and Switch, UPS etc. as per Annexure – C41: BOM-HW (Technical Bid).

viii. Certificate to the effect that the offered/quoted products conform to the tender specification.

ix. Any other document which the Bidder may consider necessary and relevant to support the quoted product/bid.

xi Quality Testing and benchmark results.

xii Attorney or authorization letter from company Secretary of bidder to sign the bid.

xiii Profit & loss account statement.

xiv Balance sheet from CA.

xiii. **Self- Certificate to the effect that the bidder/OEM has never been black listed by any Central/State Government Ministry/ Department/ office/ PSU. (Annexure C40)**

xiv. The Bidder should have a back-to-back support arrangement with OEM for support of all offered product **Annexure C5 to C38**. **A Letter from OEM/Principle Manufacturer (Annexure C39) needs to be furnished along with the Technical bid ensuring the support** atleast **for 5 years 6 months from date of supply or atleast 5 years from date of installation of ordered systems to ORGI. OEM should be accessible through e-mail/phone/VC, for support directly or through the Bidder for any support related issues.**

a. Documents to be submitted along with the Financial Bid (E3):

The financial Bid submitted by the bidder should contain bundled price information for bill of material (BOM) as quoted in technical bid with part number, make and model as per Annexure-C41: BOM-HW for all technical Annexure C5 to C38 as per Annexure-D2 (Price Schedule) format for products with 5 years comprehensive warranty, installation and rates of resident engineers. For 3 Major Data Centers, (i) NDC, Shastri Park, Delhi (ii) Lucknow (iii) Bengaluru, there would be three shifts and additional 2 Engineers per shift would be required for 8 hours shift for two years. So total 6 extra skilled engineers would be required having following skill sets (i) Server and Storage (ii) Network and Security, for management, monitoring and operations of Network & Security Services alongwith Storage and server management at each location mentioned above, as per Annexure-D2. The Resident Engineer RE-1 would be mainly for 3 Data centres mentioned above and RE-2 for 18 DCCs. To ensure 24 x 7 deployment of RE-1 (at 3 Data Centres), total RE-1 will be 24, to cover up the weekly-off in rotational basis.

Note: List of enclosures in all above bids to be submitted properly numbered and indexed along with signatures of the representative of **OEM/bidder duly authorized by an attorney or Company Secretary of quoting OEM/Bidder**. Alterations if any in the

tender should be attested properly by the representative of bidder duly authorized by an attorney or company Secretary, failing which the tender is liable to be rejected. Printed terms and conditions of the bidders will not be considered as forming part of their Bid. If the bid is not accompanied by all the above mentioned documents, the same would be rejected. **Undertaking for subsequent submission of any of the above document will not be entertained under any circumstances.**

b. Contents of Bid

The Bids prepared by the Bidder shall comprise of the following two components:

a) Technical Bid with required information and documentation along with the Earnest Money Deposit of the required amount and following as per the formats provided in the RFP.
   1. All the documents prescribed in support of Eligibility Criteria as prescribed under Pre-Qualification
   2. Bidders Particulars
   3. Bid Form
   4. Technical Specifications of the equipments
   5. Statement of Deviations from Technical Specifications
   6. Statement of Deviation from RFP Terms and conditions
   7. Schedule of Delivery
   8. Undertaking by the Bidder
   9. All technical brochures/documents relevant to the Bid
   10. Check list of Technical Bid

b) Commercial Bid to be filled in accordance with the formats provided in the Annexure-D2: Financial Bid Format

c. Key Requirements of the Bid

i. Registration on e-Procurement Platform

Bids must be submitted online through e-portal ttp://eprocure.gov.in).on or before the stipulated time mentioned in the Fact Sheet. ORGI/DCO does not take any responsibility for the delay caused due to non-availability of internet connection or network traffic jam for online bids No bid will be accepted after the said date & time for submission of the bid.

Instructions to Bidders for Registration on e-Procurement Platform

1) In order to participate in e-procurement platform the vendor should register (if not already registered) on e-procurement platform of GNCTD after paying the registration fee
2) The vendor should have class – II Digital Certificate.
3) For any clarification on e-Procurement System, please contact at Help Desk number (011- 23813523-24) and email e-proc@nic.in

ii. RFP Document Fees

RFP can be downloaded free of cost from e-Procurement portal https://eprocure.gov.in or ORGI web site www.Censusindia.gov.in

iii. Earnest Money Deposit (EMD)

a) Bidders shall submit the EMD amount of Rupees Two crore only in the form of Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any of the Commercial Banks in favour of "**Pay and Account Officer (Census)**", payable at New Delhi. The bid security should valid for a period of 45 days beyond the final bid validity period. In case of expiry of validity period of EMD, Fresh EMD to be resubmitted at least 10 days prior to expiry.

b) The EMD instrument in original has to be submitted to Joint Director (HO), 1st floor, A wing, NDCC-2 Building, Jai Singh Road, New Delhi – 110001, and copy of the same needs to be **uploaded before the due date and time of bid submission**, failing which the bid shall be summarily rejected. A scanned copy of the instrument DD/BC/PO or exemption certificate in case of NSIC or exempted category has to be uploaded along with clear scanned copies of required documents to substantiate the claim towards their credentials along with the tender documents in the appropriate space.

c) EMD of all unsuccessful bidders would be refunded by ORGI within 45 days of the bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful bidder would be returned upon submission of Performance Bank Guarantee.

d) The EMD amount is interest free and will be refundable to the unsuccessful bidders without any accrued interest on it.

e) The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.

f) The EMD may be forfeited:

i. If a bidder withdraws its bid during the period of bid validity.

ii. In case of a successful bidder, if the bidder fails to submit the performance bank guarantee and/or sign the contract in accordance with this RFP.

iv. Submission of Proposals

a) The bidders should upload the completed bids on the Government e-Procurement portal https://eprocure.gov.in).

b) The Response to Pre-Qualification criterion, Technical Proposal and Commercial Proposal should be uploaded respectively.

c) Please Note that Prices should not be indicated in the Pre-Qualification Proposal or Technical Proposal but should only be indicated in the Commercial Proposal.

v. Authentication of Bids

A Proposal should be accompanied by a power-of-attorney in the name of the signatory of the Proposal issued by the company.

vi. Right to Terminate the Process

a) ORGI may terminate the RFP process at any time and without assigning any reason. ORGI makes no commitments, express or implied, that this process will result in a business transaction with anyone.

b) This RFP does not constitute an offer by ORGI. The bidder's participation in this process may result ORGI selecting the bidder to engage towards execution of the contract.

2.6. Preparation of Proposal

i. Proposal Preparation Costs

The bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/ presentations, preparation of proposal, in providing any additional information required by ORGI to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process.

ORGI will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

ii. Language

The Proposal should be filled by the Bidder in English language only. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Bidders. For purposes of interpretation of the Proposal, the English translation shall govern.

The bids submitted by telex/telegram/fax/e-mail etc. shall not be considered. No correspondence will be entertained on this matter.

2.7 Evaluation Process

a) ORGI shall constitute a Technical Purchase & Evaluation Committee (TPEC) to evaluate the responses of the bidders.

b) The TPEC constituted by ORGI shall evaluate the responses to the RFP and all supporting documents / documentary evidence. Inability to submit requisite supporting documents / documentary evidence, may lead to rejection.

c) The decision of the TPEC in the evaluation of responses to the RFP shall be final. No representation in this regard will be entertained.

d) The TPEC may recommend for rejection of any or all proposals on the basis of any deviations.

e) Each of the responses shall be evaluated as per the criterions and requirements specified in this RFP.

f) If there is any dispute or confusion on the configuration/specification or any other general terms & conditions mentioned in the RFP, then TPEC is having the mandate

to take a decision with the approval of competent authority. TPEC may grant relaxation/deviation judiciously, in any terms & conditions and/or specification/configuration mentioned in the RFP for SI-H.

g) In case any bid is rejected by the competent authority, the concerned bidder may request ORGI to disclose the reason of rejecting the bid. ORGI shall convey the reason to concerned bidder.

2.8 Tender Evaluation

a) **Tender Validity:** The offer submitted by the Bidders should be valid for minimum period of 120 days from the date of submission of Bid.

b) Initial Bid scrutiny will be held and incomplete details as given below will be treated as non- responsive, if Proposals:
   1) Are not submitted in as specified in the RFP Document
   2) Received without the Letter of Authorization (Power of Attorney)
   3) Are found with suppression of details
   4) With incomplete information, subjective, conditional offers and partial offers submitted
   5) Submitted without the documents requested in the checklist
   6) Have non-compliance of any of the clauses stipulated in the RFP
   7) With lesser validity period
   8) Received without EMD

c) All responsive Bids will be considered for further processing as below:
   ORGI will prepare a list of responsive bidders, who comply with all the Terms and Conditions of the Tender. All eligible bids will be considered for further evaluation by a Committee according to the Evaluation process define in this RFP document. The decision of the Committee will be final in this regard.

SECTION III: QUALIFICATION & EVALUATION METHODOLOGY

The Prospective bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the requirements, as described in the RFP document. Keeping in view the complexity & volume of the work involved, the following criteria are prescribed as pre-qualification criteria for Prospective bidder interested in undertaking the Project. The Prospective bidder must also possess the technical know-how and the financial implications that would be required to successfully implement the System and support services sought by the ORGI/DCO, for the entire period of the Contract. The invitation for bids is open to all entities registered in India who fulfill prequalification criteria as specified below:

3.1 SI-H should either be:

The Original Equipment Manufacturers(OEM) of quoted equipment, who has presence in India for minimum 5 years and should be registered as company in India (minimum five years) for supply of goods and services of OEM's equipment i.e. Server, Storage, Workstations, Network, Security devices and Modular UPS. Bidders should have branch office in minimum 9 locations out of 18 RGI locations, GST number of same to be submitted along with E-2 Eligibility and Technical Bid.

3.2 If the OEM as per above is not quoting directly:

Then OEM can authorize upto 5 bidders. The bidder should be an authorized partner of the OEM (for minimum 1 year) for quoting their products in India. OEMs should have presence in India for a minimum of 3 years. Authorized Partner should have presence in India for minimum 5 years and should be registered as company in India (minimum five years). In that case, bidder should attach a letter of authorization from the original equipment manufacturer (OEM) for quoting on their behalf in this tender as shown in Annexure C39: Manufacturer's Authorization Format. Bidder must quote for Server & Storage from a Single OEM. An authorized bidder cannot quote for two OEMs for same type of equipment. If an authorized bidder quote for two OEMs or two options for same type of equipment, the bid will be rejected.

3.3 The bidder's annual turnover:

From sale of IT equipment and related systems/services should be at least Rs.300 Crores (Rupees Four Hundred Crores) during the past three years (as on 31/03/2019) in India. The audited Profit & Loss account statement should be attached for depicting above turn over. The bidder's balance sheet/certificate should show profit for past three consecutive years.

3.4 Bidder should have the following statutory requirements:

i) GSTIN number
ii) Copy of IT returns for the past three years
iii) Registration number of the company
iv) PAN number the company
v) Copy of Article of Association/Partnership deed.
vi) GST number of more than 9 offices in the specified locations out of 18 RGI mentioned locations.
vii) ISO Certificates: ISO-9000, ISO-20000, ISO 27001

The bidder must enclose attested copies of above document failing which the bid may be rejected.

3.5 Pre-Qualification for Bidder

S.No.	Description	Basic Requirement	Specific Requirements Documents
1	Legal Entity	The Bidder should be a Company/ Firm registered under the Indian companies act, 1956 (or) a firm registered under the Limited Liability Partnership Act,2008 (or) a firm registered under the Partnership Act,1932 and should be older than five years as on 31st March 2019. The Bidder should be a stable company and should not have been acquired or change of ownership in last three years.	Valid documentary proof of: Certificate of Incorporation, Certificate of Commencement, Undertaking for no change of ownership or acquisition.
2	Financial Turnover	The bidder should have an average annual turnover of at least Rs.300 crore for last 3 financial years. Certified Copy of Audited Profit & Loss account and Balance Sheet of the last three financial years, upto 31.03.2019. NB: In case Bidder is a wholly owned subsidiary, the financial experience of Parent company would not be considered for eligibility.	Certified Copy of Audited Profit & Loss account and Balance Sheet of the last three financial years, as on 31.03.2019. CA's/Company Secretary Certificate separately for the turnover from Setting up of Data Centre and Supply, Operation & Maintenance of IT Equipment
3	Financial Net Worth	The bidder should have a Positive Net Worth continuously for the last three years as on March 31, 2019 and should be profitable for each of the last three financial years.	Certified Copy of Audited Profit & Loss account and Balance Sheet of the last three financial years, CA's Certificate for Net Worth with CA's Registration No. & Seal, highlighting the requisite figure related to positive net worth profitability.
4	Tax registration and GST	Apart from company registration, all bidder must have valid Goods and Services Tax Registration (GST) Certificate and Income Tax Return The bidder should furnish following information i. COI ii. MOA & AOA iii. GST No iv. Income Tax / PAN Number.	Valid documentary proof of: i. Certificate of Inc. ii. Memorandum of Association & Articles of Association iii. GST registration document. iv. Income Tax registration / PAN Card.
5	Project Experience	During the last three years, the Bidder must have implemented/ Completed 3 similar projects, in any Govt./PSU/ BFSI Organizations in India and having into this business for last 5 years in India. Similar projects: Data Centre Establishment, Operations & Maintenance, Security, Supply of ICT/IT Equipment, SOC Establishment, Operation, Maintenance & Services	Copy of work order(s) / Purchase Order/ Completion Certificate/ contract agreement. Supported with relevant documentary evidences for the design parameters and completion certificate/copy of the final bill alongwith customer contact details including contact person name, email and phone number.
	Data Centre Establishment and Maintenance	Single order of value 70 Crore or more; OR Two orders each having minimum value of 40 Crores or more; OR Three orders each having minimum value of 30 Crores or more in past five years upto 31/03/2019.	
	Data Centre Security	Single order of value 25 Crore or more; OR Two orders each having minimum value of 15 crores or more, in past five years upto 31/03/2019.	
	Security Operation centre	The bidder must have successfully completed at least two Captive Security Operation Centre (SOC) projects in past five years as on march 31, 2019.	

6	Mandatory Undertaking	The Bidder shall: a) Not be insolvent, bankrupt or being wound-up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons; b) Not have, and their directors and officers not have, been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a Data Centre Implementation contract within a period of three years preceding the commencement of the present RFP process, or not have been otherwise disqualified pursuant to debarment proceedings; c) Not blacklisted with any of the Govt./ PSU/ BFSI as on the date of submission of the bid.	Self-Certification/ Declaration duly signed by authorized signatory on company letter head.
7	Regional Office Presence	The bidder must have office in more than 9 ORGI locations (refer Annexure-L)	GST certificates for respective locations.
8	Certifications	The Bidder must hold following Certificates at the time of submission of bid. a. CMMi Level-3 or higher b. ISO 9000 c. ISO 20000 d. ISO 27001	Copy of Valid Certificate.

3.6 Integrity Pact:

i) The Bidder should submit the undertaking as provided in Annexure-S, that it has not given offered or promised to give, directly or indirectly, any gift, consideration, reward commission, fees, brokerage or indecent to any person in service of the ORGI or otherwise in procuring the Contracts or forbearing to do or for having done of forborne to do any act in relation to the obtaining or execution of the present Contract or any other Contract with the Government of India for showing or forbearing to show favour or disfavour to any person in relation to the present Contract or any other Contract with the Government of India.

ii) Any breach of the aforesaid undertaking 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 offers by the Bidder or anyone employed by him or acting on his behalf, as defined in Chapter IX of the Indian Penal Code, 1860 or the Prevention of Corruption Act, 1986 or any other Act enacted for the prevention of corruption shall entitle the ORGI to cancel the contract and all or any other contracts with the Bidder and recover from the Bidder the amount of any loss arising from such cancellation.

iii) A decision of the ORGI or his nominee to the effect that a breach of the undertaking had been committed shall be final and binding on the Bidder. Giving or offering of any gift,

bribe or inducement or any attempt at any such act on behalf of the Bidder towards any officer/employee of the ORGI or to any other person in a position to influence any officer/employee of the ORGI for showing any favour in relation to this or any other contract, shall render the Bidder to such liability/penalty as the ORGI 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 ORGI.

3.7 Technical Qualification Criteria

The shortlisted Prospective bidder will be further evaluated based on their technical strength and capabilities in providing the services necessary to meet the requirements, as described in the tender documents.

The Prospective bidder/s meeting the eligibility criteria would be required to make a presentation of the project understanding and proposed solution submitted by them. The technical presentation should be in line with the requirements specified in Technical Evaluation Criteria. The eligible Prospective bidder/s would be intimated of the time and venue of the presentation through email. Followed by the presentation, the Tender Purchase & Evaluation Committee (TPEC) will undertake a detailed evaluation of the Technical bids.

S.No.	Technical Evaluation Criteria	Maximum Marks	Documents Required
	Bidder's Profile		
1	Average annual turnover of the Bidder per annum during the last three (03) financial years as on 31/03/2019. Marks shall be allotted as given below: >=INR 900 Crore = 15 Marks >=INR 600Crore = 12 Marks >=INR 300 Crore = 8 Marks	15	Certificate from the Chartered Accountant / Company Secretary/Statutory Auditor clearly specifying the annual turnover for the specified years.
2	Bidder should have direct presence in locations mentioned in Annexure-L: all 18 Locations = 15 Marks >=13 locations = 12 Marks >=9 locations = 8 Marks	15	Declaration must be submitted on Letter Head along with relevant certification and contact details.
3	Purchase Order for Data Centre Establishment and Maintenance for Govt/ PSU/ BFSI: Two Purchase order >= 70 Crore = 15 Marks. Single Purchase order >= 70 Crores = 13 Marks. Two Purchase order >= 40 Crore = 11 Marks. Three Purchase order >= 30 Crore = 8 Marks.	15	Customer PO along with completion certificate / copy of the final bill / Installation signoff
4	Purchase Order for Security Components in Data Centre for Govt / PSU / BFSI: Two Purchase order of >= 25 Crore = 15 Marks Single Purchase order of >= 25 Crores= 12 Marks Two Purchase order of >= 15 Crore = 8 Marks	15	Customer PO along with completion certificate / copy of the final bill / Installation signoff
5	Bidder should have executed at least 2 Captive SOC for Govt / PSU / BFSI: >3 SOC Projects = 5 marks >1 SOC Projects = 3 marks	5	Customer PO along with completion certificate / copy of the final bill / Installation signoff

Solution Presentation, Approach & Methodology			
6	Data Centre Components (Server & Storage and any one from Workstation or Networking) from Single OEM = 20 Marks from Different OEM = 15 Marks	20	Bidder's Technical BoQ, declaration with MAF's
7	Technical Submission and Presentation on Implementation Plan (should cover Solution Architecture, scalability, Interoperability and modularity features considering the future expansion of the project and the detailed project execution of plan for completing it on time)	15	Presentation to Tender Purchase & Evaluation Committee (TPEC). Each Member of TPEC will award marks individually and then average of all members will be taken up.

S.No.	Resource	Skill Set
1	2 nos. Service Engineer (RE-1) in each shift (for 24 X7) operation at each of the 3 Main Data Centres.	Engineering Graduate / MCA
		One engineer certified from Proposed OEM for Compute and Storage Solution with Microsoft & Linux certification
		One engineer certified from Proposed OEM for Security (Firewall/ NIPS)
		Over 5 years of experience in respective domain
		Good communication skill
2	1 no. Resident Service Engineer (RE-2) for general shift operation at each of the 18 Data Capture Centres, and NDC, ORGI (3 shift duty only during specified period/urgency)	Engineering Graduate/ MCA / BCA with MS certification or network certification
		Over 5 years of experience in Datacentre environment
		Good communication skill

a) Each Technical Bid will be assigned a technical score out of a maximum of 100 as per the criteria specified above.

b) Technical submission and presentation (S.No.7 of Technical Qualification) is a qualifying phase and each bidder must get minimum 5 marks out of 15 marks to qualify.

c) Minimum absolute technical score to qualify for Technical Bid is 65.

d) ORGI decision in this regard shall be final, and evaluation of Technical Proposals by TPEC shall not be questioned by any of the prospective bidder(s).

e) Although, separate marks have not been earmarked for Category-wise numbers of required & experienced manpower, but, it is mandatory. In case, the bidder fails to provide mandatory numbers of manpower having prescribed qualification and years of experience, it will be disqualified in Technical Criteria.

3.8 Technical Evaluation

a) Technical Bids will be evaluated as per the "**Annexure A2: Evaluation Mechanism"** by duly constituted Tender Purchase Evaluation Committee(TPEC) will shortlist Technical Bids on the basis of technical parameters including visit to inspect manufacturing/service/supply facilities/capabilities and evaluation of equipment.

b) For Technical evaluation, bidders have to ensure the availability of appropriate specialist, along with every type of documentation required, from their organization for interacting with TPEC and evaluation team. **The bidders will also have to make a presentation before TPEC at New Delhi for deployment of various items and methodology of implementation as per schedule communicated separately through e-mail on e-mail address mentioned in the bid.** In case a bidder does not make available the required specialist/offered product along with proper documentation/presentation, then such defaulting bidder shall be taken off the **tender** evaluation process and the bid will stand rejected.

c) A duly constituted Tender Purchase and Evaluation Committee (TPEC) will shortlist Technical Bids on the basis of technical parameters and features offered

3.9 Financial Bid Evaluation & Award Criteria

a. The Financial Bids of technically qualified Bidders will be opened on the prescribed date as advised subsequently.
b. The Bidder with lowest qualifying financial bid (L1) will be declared successful bidder as mentioned in Row F of Price Bid.
c. Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
d. In case L1 does not accept the Letter of Intent (LOI), then TPEC will decide the further course of action.
e. Quoting incredibly low value of items/GT with a view to subverting the tender process shall be rejected straight away and EMD of such Bidder will be forfeited.
f. Only fixed price financial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
g. Any conditional bid would be rejected
h. Errors & Rectification: Arithmetical errors will be rectified on the following basis: “If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail”.
i. No inquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the TPEC/its authorized representative and office of ORGI can make any enquiry/seek clarification from the bidders, which the bidders must furnish within the stipulated time else bid of such defaulting bidders will be rejected.
j. No inquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the TPEC/its authorized representative and office of ORGI can make any enquiry/seek clarification from the bidders, which the bidders must furnish within the stipulated time else bid of such defaulting bidders will be rejected.

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

ORGI reserves the right to accept or reject any proposal, and to annul the tendering process / Public procurement process and reject all proposals at any time prior to award of contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for ORGI action.

3.11 Notification of Award

Prior to the expiration of the validity period, ORGI will notify the successful bidder in writing or by fax or email, that its proposal has been accepted. In case the tendering process / public procurement process has not been completed within the stipulated period, ORGI may request the bidders to extend the validity period of the bid.

The notification of award will constitute the formation of the contract. Upon the successful bidders furnishing of Performance Bank Guarantee, ORGI will notify each unsuccessful bidder and return their EMD. The EMD of successful bidder shall be returned only after furnishing of Performance Bank Guarantee and signing of Contract.

3.12 Performance Guarantee

ORGI will require the selected bidder to submit an irrevocably, unconditionally One Single Deposit in the form of Performance Bank Guarantee (PBG) in favour of "Pay and Account Officer (Census), New Delhi, within 15 days from the Notification of award, for a value equal to 9% of total contract value. PBG should remain valid for 66 months after date of acceptance by ORGI. Extension of validity of PBG, if required, should be 45 days before its expiry. The selected bidder shall be responsible for extending the validity date and claim period of the PBG as and when it is due on account of non-completion of the project and Warranty period. In case the selected bidder fails to submit PBG within the time stipulated, ORGI at its discretion may cancel the order placed on the selected bidder without giving any notice. ORGI shall invoke the PBG in case the selected Vendor fails to discharge their contractual obligations during the period or ORGI incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions.

3.13 Signing of Contract

It is assumed that successful bidder would be signing the Service Level Agreement (SLA) with ORGI before getting the final order from ORGI. After ORGI notifies the successful bidder that its proposal has been accepted, ORGI shall enter into a contract, incorporating all clauses, pre-bid clarifications and the proposal of the bidder between ORGI and the successful bidder.

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

Failure of the successful bidder to agree with the Draft Legal Agreement and Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the award, in which event ORGI may award the contract to the next best value bidder or call for new

proposals from the interested bidders. In such a case, ORGI shall invoke the EMD of the most selected bidder.

3.15 Project Timelines

Delivery, Installation and Maintenance Schedule

S.NO.	Activity	Maximum Period Allowed
1	Delivery Period	8 weeks from the date of purchase order
2	Installation Period	45 days(6 weeks) from the date of handing over of the site for installation
3	Time available to repair/replace the faulty system during warranty period	Within maximum period of 24 hours of lodging complaint.

On the receipt of the Purchase Orders, the Bidder shall obtain all the necessary documents for the State Entry Permit in respective States wherever required by them, for complete, safe and timely delivery of the ordered products. If the Bidder is not able to supply the ordered items completely within the specified period, the EMD/Performance Bank Guarantee may be forfeited in full. Besides legal action shall be taken separately. ORGI may place location wise orders and quantity may change depending on the requirement.

The bidder is expected to install, uninstall any hardware/ software, any number of times during the contract with No extra charges

A. Delivery Process

All aspects of safe delivery including intact position of the seal for not being tampered shall be the exclusive responsibility of the Bidder. At the destination Site, the cartons will be opened only in the presence of ORGI representative and Bidder's representative. The Bidder should deliver and install all the items at specified site without any additional charge.

It may be noted that all the items as per Purchase Order shall be delivered and installed as per the schedule mentioned in "**Annexure B3: Delivery, Installation and Maintenance Schedule".** Though Purchase order of ORGI will provide all the necessary documents for ensuring smooth delivery of goods at the respective destinations, it is the responsibility of the Bidder to deliver the goods in time.

B. Penalty Calculation Process

a. Any unjustified and unacceptable delay beyond the delivery and installation schedule as per purchase order will render the Bidder liable for penalty at the rate as mentioned in the **"Annexure B4: Penalty"**

b. Penalty will be charged on the full value of the Purchase Order if the purchase

order is for single location delivery and installation.

c. In case of multi-location Purchase order, if the delivery is completed within the prescribed delivery schedule in respect of minimum 80% locations, the penalty will be charged on the NOT completed locations i.e. penalty will be charged on the remaining locations on pro-rata basis.

d. In case of multi-location Purchase order, if the installation is completed within the prescribed installation schedule in respect of minimum 80% site ready locations (if the site is not ready, a certificate is to be issued by ORGI/concerned DCOs) the penalty will be charged on the NOT completed site ready locations i.e. penalty will be charged on the remaining site ready locations on pro-rata basis.

C. Installation Process

During installation at site, if any item is found to be defective, damaged or broken, it will be replaced with new one by the Bidder at its own cost and risk within 30 days from the date on which the Bidder has been informed of such damage. Installation Certificate copies duly signed by the user should reach ORGI Headquarters along with the bills. In case of UPS, the scope of installation includes testing, integration and commissioning of true On-line double conversion, fully latest technology based Modular UPS systems as per specifications. The offer should include the details of design, manufacturing, fabrication, assembly, packing, transportation, delivery at site, unloading, erection, integration with related equipment, and putting UPS systems together with all accessories and auxiliaries as specified, in a fully operational condition acceptable to ORGI. The bidder will be responsible for engineering and providing all materials, equipment and services which are required to fulfill the intent of ensuring operability, maintainability, completeness and reliability of the total work covered within his quoted price. The bidder will be responsible for supply, laying/installation, testing and integration of the Input/output cables, switch gears including panels etc. complete as required at site. Generally, the LAN cabling work will be carried out by ORGI/DCOs. **However, at the time of installation, if additional cabling/patch chord etc. are required, the same will be done/arranged by SI-H. The price for per nodes should be mentioned separately & not part of BOQ.**

D. Testing/ Inspection Process

a. The systems must be supplied in full as per ordered configuration for acceptance. No system with short supply or alternate to the quoted product with different technical specifications shall be taken up for conduct of acceptance testing under any circumstances.

b. Failure to fulfill any of the aforementioned conditions will entail cancellation of the Purchase Order along with forfeiture of the EMD/Performance Bank Guarantee. Further, ORGI can procure same items from alternate sources at

the risk and cost of the defaulting Bidder.

c. During contract, on subassembly level if any item's specifications/model changes and becomes non available due to obsolescence/up-gradation of technology, Bidder within already approved cost may offer the item with equivalent or having better features in terms of performance and specifications. The item(s) so offered may be evaluated at ORGI/any other site as decided by ORGI for its suitability and acceptance, if considered necessary.

d. ORGI reserves the right to reject any item, if found unsuitable and /or not conforming to the approved specifications. The rejected items, if any, shall have to be taken back and replaced by good items forthwith at the cost of the Bidder. No payment will be made for rejected items.

e. It shall be the exclusive responsibility of the Bidders (SI-H) supplying the Systems to provide appropriate device drivers/software and solutions for these systems for various software platforms etc.

f. The SI-H shall provide the quality control certificate issued by respective OEM.

g. ORGI in view of projects requirement may reject any tender(s), in which any prescribed condition(s) is/are found incomplete in any respect and at any processing stage. The Bidder should provide atleast One Hard copy of System manual and User manual at each location along with electronic copy with each System, irrespective of the fact that more than one system may be meant for any location

E. Onsite Comprehensive Warranty Maintenance

The warranty period for the systems shall be taken into account as per the **"Annexure B1: Warranty and Services"** from the date of completion of supply of products, its successful installation/commissioning and acceptance by ORGI, including availability during warranty period the free spare parts, kits etc. Failure to provide satisfactory warranty service/support shall attract penalties as per table provided in clause 4.27(C)(d). in case of SI-H to be OEM, he would be required to enter into a comprehensive warranty maintenance contract agreement with ORGI for their items and in case of other items the selected SI-H would be required to enter into tripartite/back to back agreement with OEM of the particular equipment. For 3 Data centres (NDC, ORGI, Lucknow and Bengaluru) Uptime required is 99.95% on 24x7 on monthly basis. Up time required for 18 DCC locations is 99% on 24x7 on quarterly basis. ORGI/User may sign a formal SLA with SI-H separately.

The Bidder(SI-H) has also to provide repair services at all ordered locations, failing which the penalty @ 0.5 % of value of all hardware and software installed at that location will be charged per day for maximum thirty days. After one month in

both cases above, ORGI may make alternate arrangement without paying any amount for H/w and S/w to the SI-H for that site or deduct the same from pending payments/BG. The SI-H shall also deploy resident service engineer(s) at all locations (As per D2 Annexure) from the date of installation and acceptance of hardware and software failing which the same penalty as mentioned above shall be charged.

ORGI

SECTION IV: SERVICE LEVEL AGREEMENT

SI-H shall execute the project with complete professionalism and full commitment to the scope of work and the prescribed service levels. SI-H shall attend regular Project Review Meetings scheduled by ORGI and shall adhere to the directions given during the meeting. The Project Review meetings must be led by Senior Management of SI-H who would be dedicatedly involved during the entire term of the contract. Following responsibilities are to be executed by SI-H in regular manner to ensure the proper management of the project:

a) Finalization of the Project plan in consultation with ORGI and its consultant. Project Plan should consist of work plan, communication matrix, timelines, Quality Plan, Management Plan, etc.
b) Preparation and regular update of the Risk Register and the Mitigation Plan. Timely communication of the same to all the identified project stakeholders
c) Submission of Monthly Project Progress Reports
d) Monthly Compliance report, which will cover compliances to Project Timelines, Hardware and Software delivered, SLAs, etc.

4.1 Liabilities and Duties of SI-H

a) The SI-H agrees to and does hereby accept full and exclusive liability for the payment of any and all taxes, duties etc., now or hereafter imposed, increased or modified from time to time, in respect of works and materials and all contributions and taxes for unemployment compensation, insurance and old age pensions or annuities now or hereafter imposed by any Central or State Governmental authorities or local authorities or any other body which are imposed with respect to or covered by the wages, salaries or other compensations paid to the manpower;

b) The SI-H shall be responsible for the compliance with all obligations and restrictions imposed by the Labour Laws or any other law affecting employer-employee relationship and the SI-H further agrees to comply, and to secure the compliance of all sub-contactor's with all applicable Central, State, Municipal and local laws and regulations and requirements of any Central, State or Local Government agency or authority;

c) The SI-H further agrees to defend, indemnify and hold harmless from any liability or penalty which may be imposed by the Central, State or Local authorities by reason of any violation by SI-H or Sub-Contractor of such laws, regulations or requirements and also from all claims, suits or proceedings that may be brought against ORGI arising under, growing out of, or by reason of the work provided for by this Contract, or by third parties or by Central or State Government or Local Authority or any administrative sub-division thereof;

d) The SI-H shall comply and ensure strict compliance, by his employees and agents, of all applicable Central, State, Municipal and Local laws and Regulations, and undertake to indemnify ORGI from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited

to the claims against ORGI under Workmen Compensation Act, 1923, The Employees Provident Fund Act, 1952, The Contract Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and Regulations, etc. Shop and Establishment Act and any Labour Laws which would be amended/modified or any new Act, if it comes in force whatsoever, and all actions, claims and demands arising there from and/or related thereto;

e) The SI-H shall ensure to keep and maintain all the Statutory Registers and records as required under provisions of Contract Labour(R&A) Act,1970, Minimum Wages Act and the rules made there under, Employees Provident Fund Act, 1952 and keep the same available for inspection by ORGI and Government Authorities.

4.2 General Conditions

a) Deviations: ORGI shall have powers to make any deviations in the requirements viz., increase or decrease, which shall in no way vitiate or invalidate the contract and any such deviations, which the SI-H may be directed to do, shall form integral part of the contract as if originally provided therein, and the SI-H shall carry out the same on the same Terms & Conditions, in all respect on which it agreed to do the work under the contract;

b) Other conditions: The SI-H shall ensure that there is no loss or damage to the property of ORGI while executing the contract. In case, it is found that there is any such loss/damage due to direct/indirect negligence/non- performance of duty by any manpower, the amount of loss/damage so fixed by ORGI shall be recovered from any dues of the SI-H;

c) Replacement of Manpower: Should ORGI consider at its sole judgment that the manpower provided by the SI-H as unsuitable for the job, for whatsoever reason, ORGI will have the option to request the SI-H for prompt replacement within 15 days at the cost of SI-H;

d) Leave: ORGI will make no remuneration to the SI-H for the period of absence of any manpower from duties on working days during the month;

e) Transportation: ORGI shall not make any additional payment for transportation of the manpower for travel from home to work and back;

f) Agreement not Transferable: This Agreement is personal between ORGI and SI-H and is not assignable or transferable;

g) Compliance of Labour and other laws: SI-H shall comply with all the statutory requirements as are applicable from time to time and shall be solely responsible for fulfillment of all legal obligations under various statutes including contract labour (Regulation & abolition) Act 1970, Minimum Wages Act, Workmen Compensation Act, EPF and miscellaneous provisions Act, Shops & Establishment Act etc. The SI-H shall keep ORGI indemnified against any dues/compensation or any other liability of any nature whatsoever, due to non-fulfillment of any of the statutory provisions under any statute/byelaws/ notifications etc including industrial laws. ORGI shall have full right to recover any claim and liability incurred towards payment of any dues, compensation or cost from the SI-H and deduct it from his outstanding subsequent bills/Bank Guarantee. No payment for anything, not specifically mentioned in the contract, will be made.

h) Maintenance of Registers: The SI-H shall maintain Register of Personnel employed,

Salary Register, Deduction Register etc. ORGI or its nominees shall be authorised to inspect them, whenever, required or asks the SI-H to submit the certified documents;

i) Insurance & Other liabilities: The SI-H shall obtain and submit to ORGI, appropriate Insurance Policy for the personnel deployed under the contract to cover the risk of damage, accident/ death including third party liability before start of providing services;

j) Medi-claim Policy/ESI: The SI-H shall obtain a Group Medi-claim Policy against manpower deployed by it for indoor treatment up to an amount of Rs.50,000/- in one year for each manpower. The SI-H shall ensure to submit the copy of Medi-claim Policy against deployed manpower to ORGI at the time of commencement of work OR ESI will be applicable;

l) All the Terms & Conditions mentioned in the contract shall be as those mentioned herein and no change in the Terms & Conditions by the SI-H shall be acceptable;

m) ORGI shall not be responsible for any misinterpretation or wrong assumption by the SI-H.

4.3 Indemnity

a) SI-H shall indemnify the ORGI against all third party claims of infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied software/hardware/manpower etc. and related services or any part thereof. ORGI and its sub offices also shall stand indemnified from any compensation arising out of accidental loss of life or injury sustained by the hired manpower while working on the project;

b) The SI-H hereby indemnifies, protects and saves ORGI and holds ORGI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from the following:

(i) An act of omission or commission of the SI-H, its employees, its agents, or employees of its sub-contractors in the performance of the services provided under this Agreement;

(ii) Breach of any of the terms of this Agreement or breach of any representation or warranty or false statement or false representation or inaccurate statement or assurance or covenant by the SI-H;

(iii) Bonafide use of the deliverables and or services provided by the SI-H;

(iv) Misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project;

(v) Claims made by the employees who are deployed by the SI-H, under this contract;

(vi) Breach of confidentiality obligations of the SI-H;

(vii) Gross negligence or gross misconduct solely attributable to the SI-H or by any agency, contractor, sub-contractor or any of their employees by the SI-H for the purpose of any or all of the obligations under this agreement. The SI-H shall further indemnify ORGI against any loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on ORGI for malfunctioning of the equipment or software or deliverables at all points of time,

provided however,

(i) ORGI notifies the SI-H in writing immediately on being aware of such claim,

(ii)the SI-H has sole control of defense and all related settlement negotiations;

c) SI-H shall be responsible for any loss of data, loss of life, etc., due to acts of SI-H's representatives, and not just arising out of gross negligence or misconduct, etc., as such liabilities pose significant risk. The SI-H shall indemnify ORGI (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

1. Non-compliance of the SI-H with Laws/Governmental Requirements.
2. Intellectual Property infringement or misappropriation.
3. Negligence and misconduct of the SI-H, its employees, sub-contractor and agents.
4. Breach of any terms of Agreement, Representation or Warranty.
5. Act of omission or commission in performance of service.
6. Loss of data.

d) Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities, compensation suffered by ORGI arising out of claims made by its customers and/or regulatory authorities;

e) SI-H shall indemnify, protect and save ORGI against all claims, losses, costs, damages, expenses, action, suits and other proceedings, resulting from misappropriation of any third party trade secrets or infringement of any patent, trademarks, copyrights etc., or such other statutory infringements under any laws including the Copyright Act, 1957 or Information Technology Act 2000 in respect of any of the services/manpower provided/deployed by them to ORGI from whatsoever source, provided ORGI notifies the SI-H in writing as soon as practicable when ORGI becomes aware of the claim however

(i) The SI-H has sole control of the defence and all related settlement negotiations;

(ii) ORGI provides the SI-H with the assistance, information and authority reasonably necessary to perform the above and;

4.4 Confidentiality of the Documents and Information

a) The SI-H shall not, without ORGI's prior written consent, disclose the contents of the Contract or any part thereof including specifications, plans, drawings, patterns, samples, or any information contained therein or furnished by ORGI in connection with the performance of Contract to any person other than a person engaged by the SI-H in the performance of the Contract. The SI-H shall also obtain a non-disclosure undertaking from persons engaged for the project;

b) The provisions of Article 11(a) shall survive till termination/completion of the Contract.

4.5 Security of Census Data

a) The SI-H shall undertake that it shall not disclose or part with the census data made available in any form to it or its agents, representatives and/or employees engaged in connection with the performance of the contract. The SI-H shall also obtain an appropriate

undertaking from such persons regarding maintenance of confidentiality of census data;
b) The provisions of Article 12(a) shall survive even after termination/completion of the Contract.

4.6 Arbitration

a) Any difference or disputes arising between the parties with regard to performance/non-performance of the contract under this Agreement shall be resolved amicably by mutual consultation at the designated level of the parties in the spirit of goodwill and cooperation;
b) All disputes or differences between ORGI and the SI-H shall be settled amicably. If, however, the parties are not able to resolve them, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and award made in pursuance there of shall be binding on the parties. Any appeal will be subject to the exclusive jurisdiction of courts at Delhi;
c) ORGI and the SI-H shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract;
d) If ORGI and the SI-H are unable to resolve amicably any dispute arising out of the contract, even after a reasonably long period, then either party may require that the dispute be referred for resolution to the formal mechanisms specified herein below. These mechanisms may include, but are not restricted to, conciliation mediated by a third and/or adjudication in an agreed national forum;
e) In case any dispute between the Parties, both the parties will try to resolve the issue mutually within 20 days of dispute raised. Affected party will give notice in writing to other party indicating concern, proposed remedy to settle the issue. If the issue does not settle by negotiation in the manner as prescribed, the same may be resolved exclusively by arbitration and such dispute may be submitted by either party for arbitration within 20 days of the failure of negotiations. Arbitration shall be held in Delhi and conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof.
f) The disputes resolution mechanism to be applied shall be as follows:
   i) In case of dispute and difference arising between ORGI and SI-H related to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators, one each to be appointed by ORGI and the SI-H. The third Arbitrator shall be chosen by mutual discussion between both the Arbitrators, selected by ORGI and the SI-H;
   ii) Arbitration proceedings shall be held at DELHI, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English;
   iii) The decision of the majority of the arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceeding will be paid as determined by the arbitral tribunal. However, the expenses incurred by each party in connection with the preparation, presentation, etc., of its proceeding as also the fees and

expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself;

g) The SI-H and the ORGI agree that an Award may be enforced against the SI-H and/or the ORGI, as the case may be, and their respective assets wherever situated;

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

4.7 Jurisdiction of Courts

Subject to the provisions of Article 18, the appropriate courts in Delhi shall have the exclusive jurisdiction.

4.8 Modification of Agreement

All other terms and conditions would remain the same, as detailed in the tender document, except to the extent modified/amended by ORGI and accepted by the SI-H. Any modification to this Agreement shall be valid only if it is made in writing and signed by the authorised representatives of both the parties.

4.9 Use & Acquisition of Assets during the term

During the Term of the Agreement, SI-H shall:

i. Take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components, Deliverables used for the project and other facilities leased/owned/operated by SI-H exclusively in terms of the delivery of the services as per the CA (hereinafter the “Assets”) in proportion to their use and control of such Assets which will include all upgrades/enhancements and improvements to meet the needs of the project arising from time to time

ii. Term “Assets” also refers to all the hardware / Software / furniture / data / documentations / manuals/ or any other material procured, created or utilized by SI-H or ORGI for implementation of IT Infrastructure solution.

iii. Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) as on the date SI-H takes control of and/or first uses the Assets suitably upgraded subject to the relevant standards as stated in the bid to meet the SLAs mentioned in the contract and during the entire term of the Agreement

iv. Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of Assets and which are provided to SI-H will be followed by SI-H and any person who will be responsible for the use of the Asset

v. Take such steps as may be recommended by the manufacturer of the Assets and notified to SI-H or as may in the reasonable opinion of SI-H be necessary to use the Assets in a safe manner

vi. To the extent that the Assets are under the control of SI-H, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them

and as per the terms agreed with ORGI

vii. Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law

viii. Use the Assets exclusively for the purpose of providing the Services as defined in the contract

ix. Ensure the integration of the software with hardware to be setup and the current Assets in order to ensure the smooth operations of the entire solution architecture to provide efficient services to ORGI of this Project in an efficient and speedy manner

x. SI-H shall not use ORGI data to provide services for the benefit of any third party, as a service bureau or in any other manner

xi. Use best efforts to ensure that no lien, mortgage, hypothecation or any other charge is created over the Assets. SI-H agrees that SI-H will inform ORGI immediately if SI-H feels or comes to know that a charge may be / has been created over any Asset(s). In the event a charge is created over any of the Assets which are owned by, ORGI shall have the right to get the charge removed at the risk, cost, expense of SI-H and SI-H shall make good all losses, damages, costs, fees, cess, duties, etc. borne or suffered by ORGI due to creation of such charge and/or in removal of such charge and/or in discharging the obligations for removal of such charge.

4.10 Fraud and Corrupt Practices

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

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

a) “corrupt practice” means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of ORGI, who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such

official resigns or retires from or otherwise ceases to be in the service of ORGI, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the LOA or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of ORGI in relation to any matter concerning the Project;

b) "fraudulent practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;

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

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

e) "restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

4.11 Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected bidder or ORGI as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the contract, such as:

●Natural phenomenon, including but not limited to floods, droughts, earthquakes and epidemics.

●Acts of any government, including but not limited to war, declared or undeclared priorities, quarantines and embargos

The bidder or ORGI shall not be liable for delay in performing his/her obligations resulting from any force majeure cause as referred to and/or defined above. Any delay beyond 30 days shall lead to termination of contract by parties and all obligations expressed quantitatively shall be calculated as on date of termination. Notwithstanding this, provisions relating to indemnity, confidentiality survive termination of the contract.

4.12 Limitation of Liability

The SI-H's liability under this Agreement and /or its modifications shall be determined as per the Law in force for the time being. The SI-H (service integrator /System Integrator/ i.e. selected bidder) shall be liable to ORGI for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the SI-H and its employees, including loss caused to ORGI on account of defect in goods or deficiency in services on the part of SI-H or his agents or any person / persons claiming through or under said SI. However, such liability of SI-H shall not exceed value of submitted PBG except in cases where limitations on liability clause are

arising because of reason of death or personal injury, fraud or gross negligence.

4.13 Conflict of Interest

A bidder shall not have a conflict of interest that may affect the Selection Process or the Solution delivery (the “Conflict of Interest”). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, ORGI shall forfeit and appropriate the EMD, if available, as mutually agreed genuine pre-estimated compensation and damages payable to ORGI for, inter alia, the time, cost and effort of ORGI including consideration of such Bidder’s Proposal, without prejudice to any other right or remedy that may be available to ORGI hereunder or otherwise.

4.14 Exit Management

Exit Management Purpose

This clause sets out the provisions, which will apply during Exit Management period. The Parties of the contract shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

a) Confidential Information, Security and Data

SI (Service Integrator/System integrator /i.e. selected bidder) will promptly on the commencement of the exit management period, supply to the ORGI or its nominated agencies the following:

i. Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to Project; any other data and confidential information related to the Project;
ii. Project data as is reasonably required for purposes of the Project or for transitioning of the services to its Replacing System Integrator in a readily available format.
iii. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the ORGI and its nominated agencies, or its Replacing Vendor to carry out due diligence in order to transition the provision of the Services to ORGI or its nominated agencies, or its Replacing Vendor (as the case may be).

b) Rights of Access to Information

At any time during the exit management period, the SI-H will be obliged to provide an access of information to ORGI and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogs, archive data, live data, policy documents or any other material related to the Project.

c) Exit Management Plan

Bidder shall provide ORGI with a recommended exit management plan ("Exit Management

Plan") within 90 days of signing of the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

i. A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
ii. Plans for the communication with such of the SI, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer;
iii. Plans for provision of contingent support to the Project and Replacement Vendor for a reasonable period (minimum one month) after transfer.
iv. Plans for training of the ORGI staff to run the operations of the project. This training plan along with the training delivery schedule should be approved by ORGI. The delivery of training along with handholding support and getting the sign off on the same would be the responsibility of SI.
v. Each Exit Management Plan shall be presented by the SI-H to and approved by ORGI or its nominated agencies.
vi. During the exit management period, the SI-H shall use its best efforts to deliver the services.
vii. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Plan.

4.15 Termination of contract

ORGI may, terminate this contract in whole or in part by giving the SI-H at least three months prior written notice indicating its intention to terminate the contract under the following circumstances:

a) Termination for Default

ORGI may, without prejudice to any other remedy under this Contract and applicable law, reserves the right to terminate for breach of contract by providing a written notice of three month stating the reason for default to the SI-H and as it deems fit, terminate the contract either in whole or in part:

i. If the SI-H fails to deliver any or all of the project requirements / operationalization / maintenance within the time frame specified in the contract; or
ii. If the SI-H fails to perform any other obligation(s) under the contract; or
iii. If there is a breach of SLAs beyond a limit; or
iv. If there is a breach of representations & obligations

Prior to providing a notice of termination to the selected bidder, ORGI shall provide the SI-H with a written notice of 30 days instructing the SI-H to cure any breach/ default of the Contract, if ORGI is of the view that the breach may be rectified.

On failure of the SI-H to rectify such breach within 30 days, ORGI may terminate the contract by providing a written notice of three months to the SI, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to ORGI. In such event, the selected bidder shall be liable for penalty/liquidated damages imposed by the ORGI. The performance Guarantee shall be forfeited by the ORGI

b) Default is said to have occurred

i. If the supplier fails to deliver any or all of the services within the time period(s) specified in the purchase order or any extension thereof granted by ORGI.

ii. If the supplier fails to perform any other obligation(s) under the contract

iii. If the agency, in either of the above circumstances, does not take remedial steps within a period of 30 days after receipt of the default notice from ORGI (or takes longer period in-spite of what ORGI may authorize in writing), ORGI may terminate the contract/purchase order in whole or in part. In addition to above, ORGI may at its discretion also take the following actions:

iv. ORGI may procure, upon such terms and in such a manner, as it deems appropriate, goods similar to the undelivered items/products and the defaulting supplier shall be liable to compensate ORGI for any extra expenditure involved towards goods and services to complete the scope of work in totality or 10% of the work order as cancellation charges whichever is higher.

c) Termination for Convenience

ORGI may in its own discretion, by provision of a written notice sent to the selected bidder, terminate the contract, either in whole or in part at any time for its convenience. The notice of termination shall specify that termination is for ORGI's convenience, the extent to which performance of work under the contract is terminated, and the date upon which such termination becomes effective. Subsequently, the pending dues and the payments up to the date of termination will be settled accordingly after deduction of applicable taxes and liquidated damages if any.

d) Consequences of Termination

In the event of termination of this contract for any reason whatsoever, ORGI is entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective continuity of the services which the Selected bidder shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/ breach, and further allow and provide all such assistance to ORGI and/ or succeeding vendor, as may be required, to take over the obligations of the SI-H in relation to the execution/ continued execution of the requirements of this contract.

e) Post termination rights and obligations of vendor
All plans, drawings, specifications, designs, reports and other documents prepared by the Vendor in the execution of the contract shall become and remain the property of ORGI and before termination or expiration of this contract the SI-H shall deliver all such documents, prepared under this contract along with a detailed inventory thereof, to ORGI. SI-H shall also deliver proper knowledge transfer as mentioned in

4.16 Application

These Terms and Conditions shall apply to the extent that they are not superseded by provisions in other parts of the RFP.

4.17 Standards

The Goods supplied under this RFP shall conform to the standards mentioned in the Technical Specifications, and, when no applicable standard is mentioned to the authoritative standards, such standard shall be the latest issued by the concerned institution.

4.18 Patent Rights

The Bidder shall indemnify the Purchase against all third-party claims of infringement of patent, trademark or industrial design rights arising from the use of the Goods or any part thereof.

4.19 Performance Bank Guarantee and Delivery Schedule

19.1 Within 14 calendar days after the receipt of notification of award of the Contract from the Purchaser, the successful Bidder shall furnish Performance Bank Guarantee to the Purchaser, which shall be equal to 10 percent of the value of the Contract.

The Performance Bank Guarantee shall be made in the form of Fixed Deposit/ Demand Draft/Bank Guarantee with any nationalized / Scheduled Commercial Banks in India pledged in the name of “Pay & Account officer (Census)” payable at New Delhi valid for a period of three months more than the stipulated project duration. In the event of non- supply, this deposit shall be forfeited to the extent of items not supplied. Further, if the purchaser has to procure the items or part of it from any other supplier because of failure to supply in full or part by the successful bidder, the difference in payment may be made good from this Performance Bank Guarantee. The purchaser, against Performance Bank Guarantee, can also make any other adjustments for default on part of seller. The EMD of the successful bidder will be returned once the Performance Bank Guarantee is complied. The Performance Bank Guarantee shall be released/returned as the case may be after the successful completion of project. No interest will be payable for the Performance Bank Guarantee by the purchaser.

19.2 Delivery and installation should be completed within 14 weeks from the date of issue of

LOI/Purchase Order.

19.3 Failure of the successful bidder to comply with the requirements shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid Performance Bank Guarantee.

19.4 On supply of the Scanners by the successful bidder it will be the property of the purchaser. Even in case the successful bidder withdraws from the contract subsequently due to any reason the equipment will not be returned.

4.20 Testing and Acceptance

Normally, testing and acceptance of equipment will be undertaken at the actual site of installation. However, if considered necessary, testing and acceptance may also be undertaken centrally at the National Data Centre, Office of the Registrar General, India, DMRC IT Park, Shastri Park, Delhi. The acceptance test will include the running of sample forms. Details of testing would be provided to the successful bidders prior to conducting the test. The installed system must give same or better performance results as shown during performance test. Failure to fulfill the above-mentioned conditions will entail cancellation of the contract alongwith forfeiture of the EMD/Performance Bank Guarantee.

4.21 Spare Parts

The Bidder will also undertake the supply and storage of necessary spare parts on sites on a continuing basis as part of warranty obligations under the contract during the five years of free Warranty Period and ensure supply of spare parts three years thereafter.

4.22 Service Facilities

The Bidder shall ensure comprehensive onsite maintenance for the scanners during free Warranty Period. The bidder should also quote separately the post-warranty annual maintenance charges and give an undertaking to maintain the equipment for another three years if so desired by the purchaser. Post warranty maintenance Charges will not be considered for comparison.

4.23 Incidental Services

The Bidder is required to rectify any bugs/shortcomings detected by the purchaser/user community in the Counting machine/Scanner/customized application free of cost.

4.24 Training

The Bidder shall provide onsite free training to officials nominated by the Purchaser on scanners being supplied by him. The details of training are as under:

S.No.	Description of module	No. of persons	Duration per batch
1.	Basic System Operations & Maintenance training onsite at 15 Data Capture Centers - One batch for 5 days at each DCC	540	5 Days
2.	(Training at 3 Main Data Centers only) Features, functionality of all the Installed Equipment, OS and Software, its customization, advanced features and maintenance etc.	60	10 Days

The trainings would be conducted at the respective sites where the successful Bidder installs the equipment. The schedules for trainings would be drawn up as directed by the Purchaser. The Purchaser will be able to extend his available training facilities for this purpose.

4.25 Proprietary rights

The Bidder shall indemnify the Purchaser against all third party claims of infringement of patent, copyright, trademark, license or industrial design rights, software piracy arising from use of goods or any part thereof in the Purchaser's country. ORGI will be the owner of all the software developed for this project by SI/Core Team.

4.26 Use of Contract Document & Information

The Bidder shall not, without the Purchaser's prior written consent, disclose the contract, or any provision thereof, or any specifications, plan, drawing, pattern, sample or information furnished by or on behalf of the Purchaser in connection therewith, to any person other than a person employed by the Bidder in the Performance of the contract.

4.27 Payment Terms

A. Payment of Hardware/software items supplied

1) A pre-receipted bills in triplicate shall be submitted in the name of "Office of Registrar General, India, New Delhi" by the selected bidder and other relevant documents, such as 5-year warranty certificate from respective OEM, and Bank Guarantee (BG) shall be submitted in the name of Pay and Account Officer(Census),New Delhi by the Bidder soon after the delivery and installation of items at ORGI specified locations along with a copy of the duly receipted Delivery Challan and Installation Certificate, duly signed by the concerned DCC Incharge/DCO with date and stamp.
2) All payment shall be made in Indian Rupees as per following schedule:
   a) 70% payment will be made on delivery and warranty certificates
   b) 20% payment after submission of installation certificate.
   c) 10% payment shall be released after one month of the Installation.
   d) The Installation of the equipment has to be completed within 45 days (6 weeks) after handing over the site.
   e) The SI-H must provide Proof of Delivery (PoD) and Proof of Installation both duly signed by the concerned DCC Incharge/DCO with date and stamp
3) The Payments of Resident Service Engineer will be made on quarterly basis from ORGI. The bills may be submitted directly to ORGI after obtaining the satisfactory

performance certificate from the concerned data center in-charge/Controlling officer of DCO.

B. Clarification on Payment

a) All payments made by ORGI shall be after deductions of tax at source, wherever applicable as per the provisions of the Income Tax Act, 1961. Other taxes and duties etc., if any, will be deducted as applicable by Law;

b) Payment shall be made after adjusting/deducting penalties etc. (if any) of the current or previous period;

c) The payment to be made to SI-H, against the deployment of each manpower per month, shall remain fixed during the period of contract. There shall be no increase in price for any reason whatsoever;

d) However, the benefits realised by SI-H due to lower rates of GST shall be passed on by the SI-H to ORGI;

e) In case, other Statutory Payables (EPF, ESI) are increased by the respective laws during the tenure of the contract, the additional cost will be borne by the SI-H only. However, changes in the GST will be borne by the ORGI;

f) The SI-H, being the employer in relation to manpower engaged/ deployed by it, to provide the services under this agreement, shall alone be responsible and liable to pay wages/salaries to such manpower, which in any case will not be less than in accordance with the minimum wages as fixed or prescribed for the category of workers employed/deployed by it, from time to time or by State Government and/or any authority constituted by or under any law;

g) Should there be a requirement for extension of services of manpower, payments shall be made as per the Terms & Conditions of the initial contract;

h) The SI-H must submit the Quarterly Bill in arrears for manpower deployed, alongwith "Manpower Deployment & Satisfactory Service Certificate" as per the format provided in Annexure-M, duly attested by concerned DCC, In-Charge. The Quarterly Bill along with the Certificate that the provisions of Minimum Wages Act and Statutory deductions of the concerned state have been adhered;

i) The ORGI will make the payment against each manpower deployed by the SI-H for the services rendered, subject to the deduction/penalty, if any.;

k) The amount include Wages and other allowances to the manpower deployed and also PF/EPF/ESI, other welfare measures/terminal benefits and other legal obligations, if any, as per Central/State Govt. rules, as amended from time to time, and SI-H would follow them;

l) Every quarter the SI-H shall Certify that the monthly salary to the manpower, deployed under this contract, have been disbursed at the time of claiming payments;

m) Whenever, any claim whatsoever, for the payment of sum of money to ORGI arises out of or under this contract against the SI-H, the same may be deducted by ORGI from any sum then due or which at any time thereafter may become due to the SI-H under this contract or from any other sum whatsoever due to the SI-H from ORGI or from his Performance Bank Guarantee, or he shall pay the claim on demand;

n) Any sum of money due and payable to the SI-H (including the Performance Bank Guarantee returnable to him) under this contract, may be withheld or retained by way of lien by ORGI, against any claim of ORGI or such other person or persons in respect of payments of sum of money arising out of or under any other contract made by the SI-H with ORGI. The sum of money so withheld or retained under this clause by ORGI will be kept withheld or retained as such by ORGI till his claim is mutually settled.

C. Penalty

a) The deduction in payment, if any (as mentioned above), will be made, except exempted by ORGI in view of the extraordinary circumstances beyond the control of the SI-H, provided that permission is sought by the SI-H, in advance and in writing with justification, to exempt the delay in providing Satisfactory Services/Performance Norms;

b) For failure of anything mentioned in the contract on behalf of SI-H by more than 30 days, may cause the termination of the contract and forfeiting of Performance Bank Guarantee/Bank Guarantee or Black listing or combination of both;

c) If the SI-H does not manage to complete the manpower requirement at required sites within a month of placement of order, or such authorised extension of period as may be permitted by ORGI in writing, ORGI shall impose a penalty @1% of the Salary component for each week's delay;

d) Penalty on account of failure to meet the deadlines for various reasons will be deducted as follows:

S.No.	Activity	Rate
1	Failure in maintaining Delivery Schedule (For unjustified and unacceptable delay)	0.20% per day of PO value subject to maximum penalty of 10%of overall value of Purchase Order. After 30 days, ORGI holds the option for cancellation of the order for pending supply, and will procure the same from any other Bidder at the cost of the supplier and may forfeit the EMD/ Performance Bank Guarantee of the Bidder. In addition, Bidder shall also be liable to pay to ORGI a cancellation charge of 8.5% (Eight point five percent) of the value of un-supplied items.
2	Failure in maintaining installation Schedule(For unjustified and unacceptable delays for site ready locations)	0.20% per day of PO value subject to maximum penalty of 10% of overall value of Purchase Order. After 15 days ORGI holds the option for cancellation of the order and get installed the same from any other Bidder at the cost of the supplier and forfeits the EMD/ Performance Bank Guarantee of the Bidder. In addition, Bidder shall also be liable to pay to ORGI a cancellation charge of 8.5% (Eight point five) of the value of un-installed items.

3	Maintenance during warranty period(For unjustified and unacceptable delays)	Penalty at the rate of 0.5% of item value per day per system will be charged/recovered from Bidder out of withheld amount towards warranty subjected to maximum of 5% (five percent) of the total order value per year will be recovered either from Performance Bank Guarantee or from any other pending payments. Any Loss thus caused will be recovered from the Performance Bank Guarantee.
4	Replacement of the faulty system	Any system failing at subsystem level at least three times in three months, displaying chronic system design or manufacturing defects or quality control problem will be totally replaced by the Bidder at his cost and risk within 30 days, otherwise penalty as per above clause 3 shall be applicable.

4.28 Modification of Tender

ORGI reserved the rights to modify/insert/delete any terms and conditions of this tender in the interest of work. This would be notified to the prospective/successful bidder through ORGI web site or by email or by appropriate means of communication as the case may be. Appropriate penalty clause will be defined by the ORGI in the Service Level Agreement.

4.29 Currency of Payment

Payment shall be made in Indian Rupees only.

SECTION V: TERMS & CONDITIONS FOR SELECTED BIDDER

5.1 Keeping in view the ORGI -project commitment, ORGI reserves the right to evolve a super-set of technically qualified accepted systems and subsystem, items of their brands and models for the entire range of systems covered by various Annexure of this **tender** so as to take care of the service delivery related aspects concerning the suitability of configuration needs matching the project requirements from time to time.

5.2 Validity of the panel is given in the "**Annexure A3: Validity of bids, rates etc."**.

5.3 In the event the Bidder's Company or the concerned division of the Company is taken over/bought over by another company, all the obligations and execution responsibilities under the agreement/empanelment with ORGI, should be passed on for compliance by the new company in the negotiation for their transfer.

5.4 Successful Bidder have to agree for honouring all **tender** condition and adherence to all aspects of fair trade practices in executing the purchase orders placed by ORGI.

5.5 In case of successful bidder is found in breach of any condition(s) of tender or supply order, at any stage during the course of supply/installation or warranty period, the action as per terms of contract, shall be initiated against the bidder and EMD/Performance Bank Guarantees shall be forfeited, besides debarring and blacklisting the bidder concerned for at least three years, for further dealings with ORGI.

5.6 The bidder should not assign or sublet the contract or any part or it to any other Bidder in any form. Failure to do so shall result in termination of contract and forfeiture of Performance Bank Guarantee.

5.7 If the name of the product is changed for describing substantially the same in a renamed form; then all techno-fiscal benefits agreed with respect to the original product, shall be passed on to ORGI and the obligations with ORGI taken by the Bidder with respect to the product with the old name shall be passed on along with the product so renamed.

5.8 The Bidder should not assign or sublet the order or any part of it to any other agency in any form. Any such eventuality shall result in termination of contract and forfeiture of Performance Bank Guarantee/EMD concerning such Bidders/parties.

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

5.10 During the validity of the bid including the extended period, if any, if the Bidder quotes, sells or exhibits written intention to sell any System or sub- system of the same or equivalent configuration to any other Department/ Organization at a price lower than the price fixed for ORGI under similar terms and conditions, the Bidder shall voluntarily pass on the price difference to ORGI. The effective date will be the date of quoting lower rates by the bidder in the bid/quote. In the event of lowering of government levies subsequent to the finalization/submission of the panel/bids, the Bidder shall automatically pass on the benefits to the ORGI.

5.11 The Bidder should have a back-to-back support agreement with OEM for support of all offered product and for which the bidder should submit all the warranty/service

certificates from all OEMs along with the invoice for the complete warranty period.

5.12 No deviations from these terms and conditions will be accepted; violation thereof will lead to rejection of the bid and forfeiture of EMD.

5.13 In case the successful Bidder is found in-breach of any condition(s) of bid or supply order, at any stage during the course of supply/installation/commissioning or warranty period, the action as per prevailing rules/laws, shall be initiated against the Bidder and EMD/Performance Bank Guarantees shall be forfeited, besides debarring and Black listing the Bidder concerned for at least 3 years, for further dealing in Govt. departments.

a. General Conditions

a) Any attempt by Bidder to bring pressure towards ORGI's decision making process, such Bidders shall be disqualified for participation in the present tender and those Bidder may be liable to be debarred from bidding for ORGI tenders in future for a period of three years.

b) Printed conditions mentioned in the bid submitted by Bidders will not be binding on ORGI unless it is agreed by ORGI under the contract. All the terms and conditions for the supply, testing and installation, payment terms, penalty etc. will be as those mentioned herein and no change in the terms and conditions by the Bidders will be acceptable.

c) Upon verification, evaluation / assessment, if in case any information furnished by the Bidder is found to be false/incorrect, their total bid shall be summarily rejected and no correspondence on the same, shall be entertained and EMD may be forfeited.

d) Termination for Insolvency: ORGI may at any time terminate the purchase order / contract by giving written notice of 4 (four) weeks to the bidder, without any compensation to the bidder, if the bidder becomes bankrupt or otherwise insolvent. ORGI will not be responsible for any misinterpretation or wrong assumption by the Bidder.

b. Miscellaneous

In the event of any dispute or difference arising under any special condition of empanelment in connection with this empanelment, the same shall be referred to Chairman, ORGI for final decision and the same will be binding on all parties. Any other terms and condition, mutually agreed to prior to finalization of the order/ agreement shall be binding on the supplier.

c. Applicable Law

The agency shall be governed by the laws and procedures established by Govt. of India, within the framework of applicable legislation and enactment made from time to time concerning such commercial dealings/processing. All disputes in this connection shall be settled in Delhi jurisdiction only. ORGI reserves the right to cancel this tender or modify the requirement. ORGI also reserves the right to modify/relax any of the terms & conditions of the tender by declaring / publishing such amendments in a manner that all prospective Bidders / parties to be kept informed about it.

Annexure – A1: Evaluation Mechanism

1. A duly constituted Tender Purchase and Evaluation Committee (TPEC) will shortlist Technical Bids on the basis of technical parameters and features offered.

2. Bidders will be technically short listed based on the Specifications matching / Technical discussions and the names of technically short listed Bidders will be announced to only those Bidders who's bids will qualify for opening the Financial/Commercial Bids.

3. For Technical evaluation, bidders have to ensure availability of appropriate specialist, along with required documentation for interacting with TPEC. If the required specialist along with proper documentation is not made available by bidders, then such defaulting bidders shall be debarred from the tender evaluation process. **The bidders will also have to make a presentation before TPEC as per schedule communicated separately through e-mail on e-mail address mentioned in the bid.**

4. Bidder must quote/offer only one option (Make/model) against each of the items listed in the **Annexure: Technical (C5 to C38).** During Technical Evaluation, no change of make and/or model of the equipment's will be allowed. Only quoted products will be evaluated/inspected.

5. The TPEC will short list the Technical bids configuration wise on the basis of technical parameters. If desired, TPEC may ask to bidders to bring one of each quoted model or improved latest model of same make as per specifications set out in the tender for technical evaluation, along with their own test and measuring equipment's/software at ORGI HQ or any other site as may be finalized by ORGI, as per schedule to be intimated to them. In case of improved model, the improved model should not be inferior in any specification than the quoted model. During Technical Evaluation the quoted product shall be physically verified for the required tender specifications, tested for reliability, functionality, benchmarked and other features as decided by the TPEC. In case the Bidder fails to bring the quoted products within the prescribed limit given by the ORGI for evaluation, the bid shall be rejected and EMD forfeited. In case TPEC decides to inspect the items at Bidder's/OEM's premises, the expenditure on travel will be borne by ORGI.

6. If during the technical evaluation, any of the System fails then no subsequent chance will be given to the Bidder. However, improved latest model of same make on account of technological trends which meets all the tendered technical specifications and superior in specifications then the quoted model, if available instantly on the spot could be considered by TPEC for evaluation. Based on the demonstration/evaluation test results, Bidders will be short listed. Financial bids of only technically qualified Bidders will be opened in their presence. In their own interest the bidders are advised to ensure that the Server, Storage, Workstation systems, Network(Routers & Switches) & Security device and UPS items brought by them for

evaluation conform to all tendered technical parameters/specifications and are functional. Systems not meeting complete tender specifications will not be considered for evaluation.

7. Specifications given in **Annexure C: Technical** are minimum specifications that are to be met. However if Bidder desires to quote higher specifications, they are free to do so.

8. **Compliance statement** to the technical specifications in the form of **'Complied'** or **'Not Complied'** should be enclosed in the technical bid. The compliance statement should contain the signature of the authorized person and the seal of the company. Any deviation should be mentioned / explained clearly in a separate sheet by the bidder.

9. If the name of the product is changed, the renamed product should have equivalent or superior technical specifications.

10. No enquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the Committee/its authorized representative and office of ORGI can make any enquiry/seek clarification from the bidders. In such a situation, the agency shall extend full co-operation. The bidders can also be asked to arrange demo of the offered systems, in a short period notice, as such the bidders have to ready for the same.

11. Bidder should score minimum 65 Marks in technical bid to qualify for commercial bid opening, refer Annexure A2 for details.

12. The bidder must quote for all annexures otherwise the technical bid will be rejected. The bidder shall be considered as technically qualified if they qualified for all annexures C5 to C38. RE-1 and RE-2

Annexure – B1: Warranty and Services

S.NO.	Description	Compliance
1	All hardware and software items should be under 5 (five) years free on-site comprehensive warranty support service from the date of acceptance including free provision of spare parts, kits etc.	
2	During warranty period besides service/ maintenance of Hardware, System/driver Software and its Peripherals, all software up-gradations, bugs/ patches and services shall be provided free of cost by the Bidder.	
3	The Bidder should fulfill the following conditions during warranty period:	
3(a)	Supplier will maintain enough spares at ordered user premises / warehouse (bidder/OEM) not less than 10% or 1 unit whichever is higher, for items e.g. HDD, keyboard, mouse and not less than 5% or one unit whichever is higher of other items so as to provide satisfactory on-site comprehensive maintenance services during the warranty period to get 99% uptime. Supplier will indicate the level of spares, which will be stored by them at user's premises for providing comprehensive on-site warranty services to User's site.	
3(b)	Bidder would provide the help desk support services through telephone/e-mail where users can lodge their complaint. Each user will be assigned a unique trouble ticket number through which he should be able to track the action taken on his complaint through a support portal. The User Coordinator at user site will maintain the list of trouble tickets being opened and closed. Toll Free No. to be provided.	
3(c)	Any failure in the equipment supplied / any accessories thereof should be rectified within maximum period of 24 hours of lodging complaint.	
3(d)	For 3 Data Centres (NDC, ORGI, Lucknow, Benagluru) Uptime required is 99.95% on 24x7 on monthly basis. Up time required for 18 DCC locations is 99% on 24x7 on quarterly basis. Penalty as mentioned in table of clause 4.27 (C)(d) will be charged or recovered	
3(e)	Any system failing at subsystem level at least three times in three months, displaying chronic system design or manufacturing defects or quality control problem will be totally replaced by the Bidder at his cost and risk within 30 days.	
3(f)	Bidder shall carryout preventive maintenance and fine-tune the performance of the system at each site at least once in every six months besides regular service during 5 years warranty and maintenance period.	
3(g)	On completion of the Warranty period, the Performance Bank Guarantee without any interest accrued shall be released after satisfying that proper free warranty support has been provided during warranty period of five years for all the systems. If considered necessary, suitable amount of penalty shall be recovered from the Bidder out of either already due payments or from their Performance Bank Guarantee while releasing the Performance Bank Guarantee.	
4	The start date of warranty will be considered from the date of acceptance by ORGI/DCOs.	
5	On completion of the Warranty Period, the Performance Bank Guarantee, without any interest accrued, shall be released after satisfying that proper free warranty support has been provided during warranty period of five years for all the systems. If considered necessary, suitable amount of penalty shall be recovered from the Bidder out of either already due payments or from their Performance Bank Guarantee, while releasing the Performance Bank Guarantee.	
6	The Bidder shall update the device drivers and other system software(s) released during five years comprehensive warranty & maintenance period without any financial implication to ORGI.	
7	Escalation Matrix of OEM & SI-H to be provided with Toll Free No.	

Annexure – B2: Services to be provided

S.No.	Description	Requirements
1	Training	The SI-H has to provide operational training to DCC staff (around 480) at 15 locations for basic commands of the Operating System, its tools, utilities and basics of network and WEB concept in one or different batches at user premises. The duration of the training shall be minimum 5 days where hands-on training sessions should also be given. In addition to above, Selected Bidder would also provide onsite training to end-user at the time of installation of equipment. The SI-H shall also provide advance training to DCC officers (around 60) for 10 days on Operating System of Server, Storage Devices, LAN/WAN, WEB, Database Operations and system administration at 19 locations.
2	Delivery of items	At the destination site, the cartons will be opened only in the presence of ORGI official and the selected Bidder's representative. Upon delivery of the equipment, selected Bidder should obtain signed proof of delivery from the ORGI/DCOs. The same shall be submitted along with the bills by the Bidder for payment.
3	Installation	Unpacking of all items and pre-installed rack, rack mounting of items, connection and configuration of all hardware, software and networking items. Upon satisfactory installation of the equipment, Bidder should obtain signed installation certificate from the ORGI/DCOs. The same shall be submitted along with the bills by the Bidder for payment. It will be the responsibility of the SI-H to make the system operational network available with the user. The successful bidder shall coordinate with network provider/LAN vendor, if required. It will be the responsibility of the SI-H to quote the product interfaces and related accessories in such a way that all items are interconnected, configured and integrated for complete operationalisation of the centre without any additional cost. For site not ready (SNR) cases, SI-H is required to submit a certificate to ORGI Hqrs., duly signed by the concerned DCOs. No penalty will be levied for SNR cases, however Bidder has to install the items within 30 days of receipt of site ready notice from user else it will attract penalty as per Annexure: Penalty. Installation Certificate copies duly signed by the concerned user should reach ORGI. During the installation process and warranty support period, SI-H must identify one Project Manager to manage and monitor entire project and should be single point of contact for any issues/ discussions at Delhi with necessary team for coordination and their sub offices.
4	Project Management	The Project Manager should be qualified person with at least 5 years of experience in handling large Projects. Once the H/w in the national data centre and at all 18 locations are operational/accepted, the SI-H shall deploy one resident service engineer for 5 years for all the 19 location, to address all hardware, software and configuration, backup issues during the warranty period. The bidder will also deploy 2 resident engineers per shift at NDC and at two DR sites for three shift operations.

Annexure – B3: Site Not Ready (SNR)

Site Not Ready (SNR) Certificate

1	Name of the state
2	Name of the location
3	Purchase Order No. and Date
4	Name of the Equipment
5	Name of SI-H
6	Date of 1st Visit
7	Site Not Ready, Reason
8	Tentative Date of Site being Ready for Installation
9	There is no delay on the part of Bidder for the installation

ORGI

Minimum Requirements for Data Centre

Considering the Data Centre is a mission critical Data Centre, the System Integrator (SI) shall therefore adequately plan for high availability of equipment's and build for the necessary operational support to maintain an uptime of 99.95% on a monthly basis. The SI should also ensure that all the equipment in the Data Centre are highly efficient at any load and appropriately maintained and managed for the project period (including extended period as applicable)

The minimum requirements/ specifications for the Data Centre are detailed in the following sub-sections. While it is mandatory for the SI to meet these minimum requirements, if the SI estimates that a particular requirement would need a higher category of equipment, the SI should provision for the same in the bid proposal. The SI should however provide basis for arriving at the solution being proposed as part of his bid.

Design Considerations

IT System Design Consideration

DC is envisaged to establish a robust infrastructure to enable the ORGI to deliver the services quickly and effectively through infrastructure implemented and managed by a competent System Integrator. The government aims to focus more on the service delivery rather than on the issues surrounding the Infrastructure.

The system design shall be able to provide logically unified and shared infrastructure flexible enough to rapidly respond to requirements and also accommodate future technology enhancements, distributed applications, database applications running on bare metal, virtualized applications running in multi-hypervisor environments.

The SI has to establish centralized DC environment that will be used to host multiple applications with simplified operations and increased application responsiveness to support a new generation of distributed applications. The system design will support following:
a. Deliver IT as a service starting with IaaS, PaaS from Go-Live phase and SaaS as per requirement of purchaser after Go-live.
b. Deliver responsive IT based services to State government/departments on demand at scale and anywhere.
c. Deliver reliable User Experience

High Level IT Infrastructure

The IT infrastructure for DC will require various set of IT components for running various applications. The SI will be responsible to Supply, Install, Configure, Test and Operate & Maintain the entire solution for the project period (including extended project period as applicable). The bidder should propose only one solution that is in accordance with the tender specifications.

The following is an indicative list of categories of components (Software, Hardware) and Services that the SI is expected to provide for supply, install, configure and test (as per BOM):

a. Computing Infrastructure such as Compute, Storage, Operating Systems and Hypervisor etc.
b. Network Infrastructure such as Routers, Switches, etc.
c. Security infrastructure such as Firewalls, ADC, WAF, SOC, DDOS etc.
d. SIEM, SAA, DLP, EDR and virtualization, etc.
e. Enterprise Class Storage, VTL, etc.
f. Disaster Recovery setup in Active-Active & Active-Passive mode.
g. Operation and maintenance Services for project period (including extended project period as applicable).

The above list is indicative only. The SI will be required to design solution which is scalable and provides for next generation latest technologies like virtualisation, layered Security, SoC etc. The SI is free to add any additional components that are deemed necessary for providing the overall solution as a whole. The SI should also consider the following while proposing the solution:

i. The SI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to the devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
ii. The purchaser will not be responsible if the SI has not provisioned for any components, sub-components, assemblies, sub-assemblies as part of bill of material in the bid response. The SI will have to provision to meet the solution requirements, at no additional cost and time implications to the purchaser.
iii. The SI should ensure that there is a 24x7x365 comprehensive onsite operations & management support for project period (i.e. 5 years) through manpower services after Go-Live for all respective components (Hardware / software) supplied by SI.
It is expected that SI shall ensure that the equipment/components being supplied will be supported by respective OEMs for minimum 5 years from date of bid submission. If any component goes out of support by the respective OEM for any reason whatsoever, the SI shall replace the same with an equivalent or higher model that is acceptable to purchaser without any additional cost and without impacting the performance of the solution in any manner whatsoever. Any components, subcomponents, assemblies, sub-assemblies (i.e. server, storage, OS) required for installation of SIEM, EMS, ADC, backup, patch management, antivirus or any other software/management software needed for IT infrastructure will be provided by SI without any additional cost.

Scalability

i. All components of the Data Centre must support scalability to provide continuous growth to meet the requirements and future demand of the State.
ii. A scalable system is one that can handle increasing numbers of requests without adversely affecting the response time and throughput of the system.
iii. The DC shall support both vertical (the growth of computational power within one operating environment) and horizontal scalability (leveraging multiple systems to work

together on a common problem in parallel).

Availability

i. All components of the DC shall ensure high availability of the applications and other Data Centre services.
ii. Designing for availability assumes that systems will fail, and therefore the systems are configured to mask and recover from component or server failures with minimum application outage.
iii. The SI shall make the provision for high availability for all the services of the Data Centre. However, application availability is the responsibility of the application owner and the SI cannot be held responsible for any problem related to application and its availability.

Interoperability

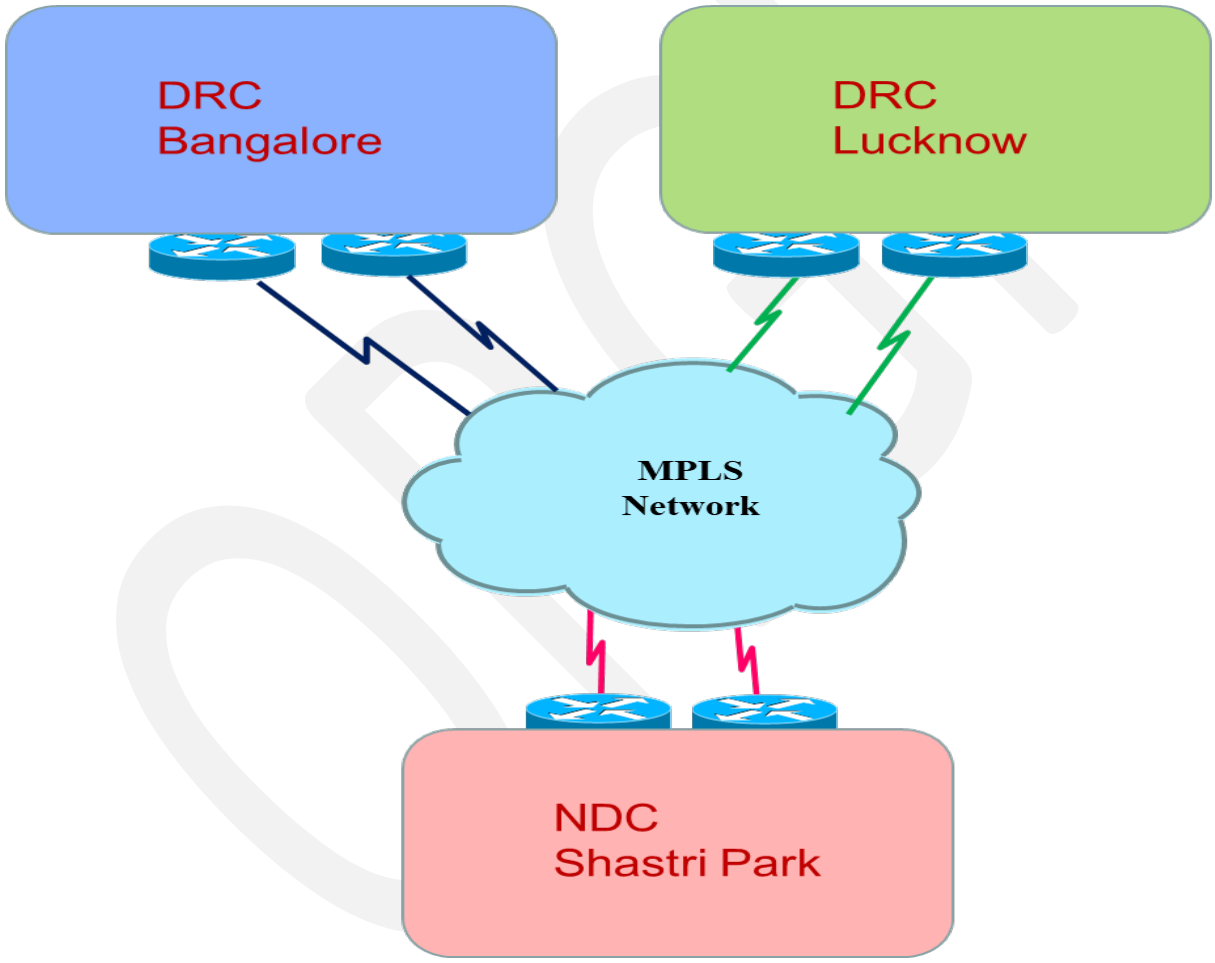
i. The entire system/ subsystem should be interoperable, in order to support information flow and integration.
ii. Operating systems and storage technologies from different OEMs must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired.

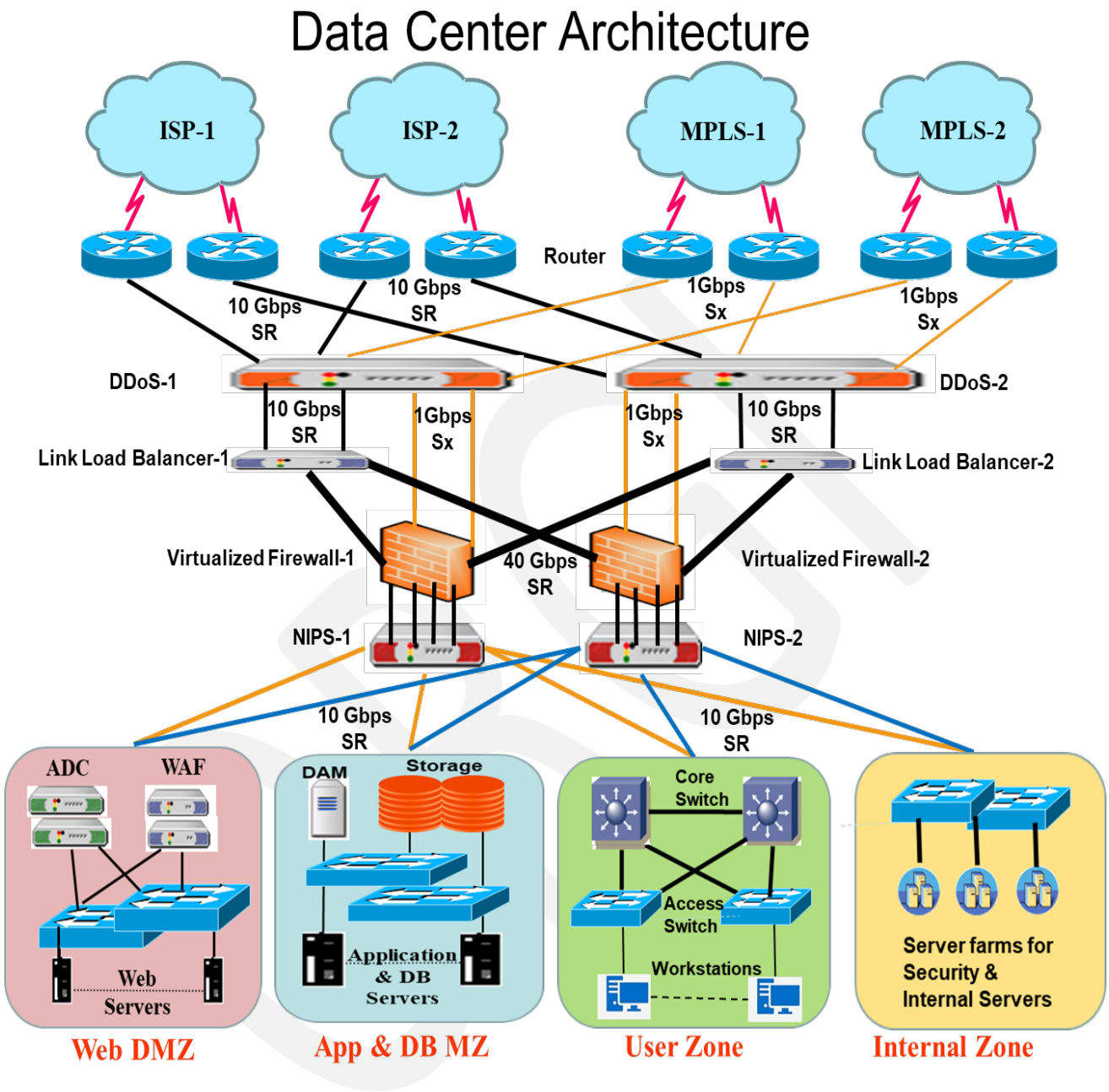
Cyber Security

i. The Data Centre must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/malicious intent.
ii. Such attacks and theft should be controlled and well supported using layered Security Approach with next generation cyber security appliances e.g. Firewalls, IPS, WAF, DDOS systems, Situational Awareness & Analytics and other infrastructure protection mechanisms.
iii. Furthermore, all the system logs should be properly stored (for minimum of 6 months or as per policy defined) & achieved for future analysis and forensics whenever desired.

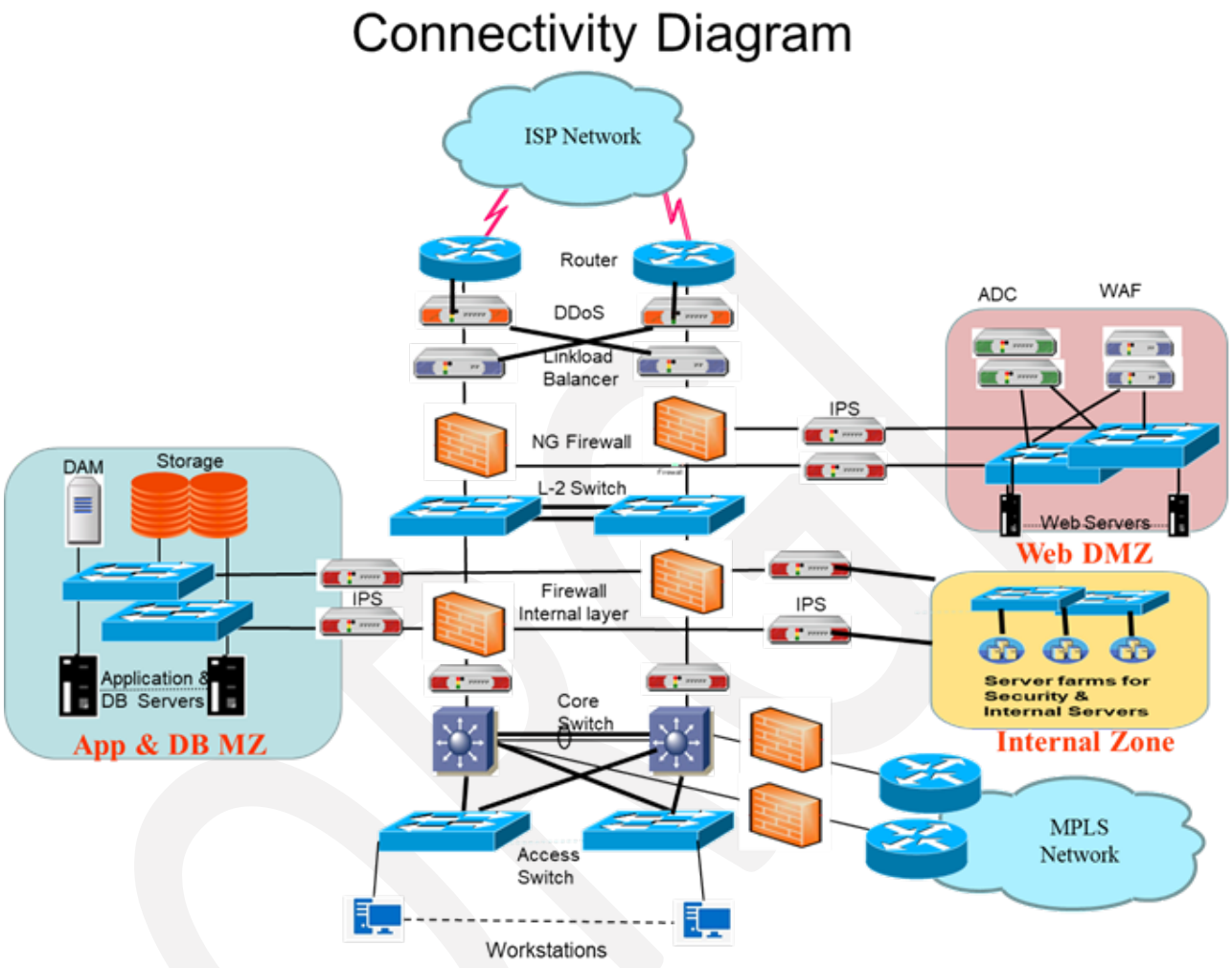
DC & DRC Architecture

Data Centre and Disaster Recovery Centre will same network and security architecture. ORGI had finalized following network and security architecture for Data center & DR locations. Data Centre and Disaster Recovery Centre will be inter-connected using MPLS cloud. Following diagram is for MPLS connectivity between three main DC's (DC plus 2 DRC).





Note: All diagrams shown in the RFP for SI-H are indicative diagrams. 18 DCCs are standalone, however 3 DCs are inter-connected



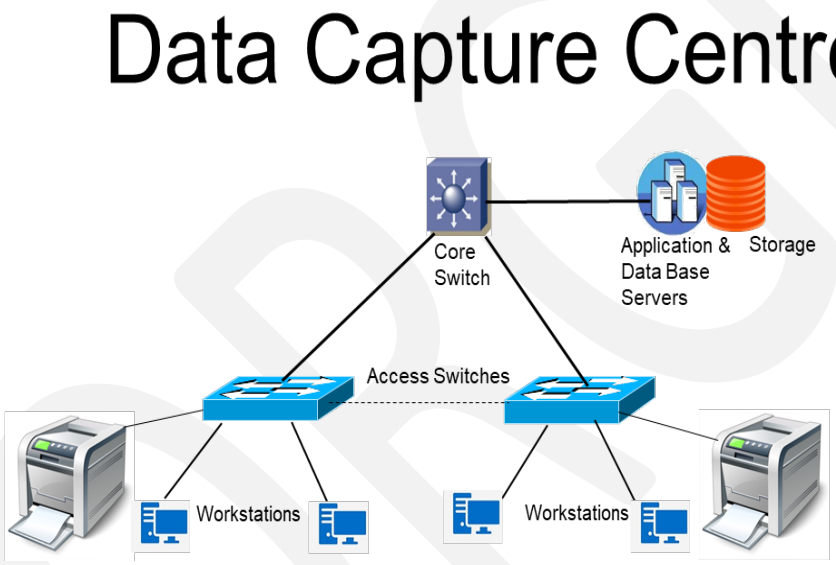
Note: Offered Solution should be complete in all senses including Hardware, Software, etc. and should comply to technical and functional specifications mentioned in Section: Technical Specifications.

If there is any software component proposed in the bid, bidder is required to quote hardware required (as per software OEM recommendation) to make it fully functional for project duration.
Layered Security approach helps in maximum security coverage, it has been decided that following different layers of security DDoS, Firewall, NIPS, and EndPoint Protection should be from different Security OEM.

Data Capture Center Architecture

Data Capture Center is stand-alone, DCC will host Couple of Application Servers, DataBase Servers and Storage housed in Chassis which will be connected to Core switch using multiple 10G links. Manned & unmanned Workstations will connect to application servers and shall perform the respective tasks. All workstations will connect to Access-Switch and Access Switch will connect to Core Switch using 10G Uplink. Other network devices like printers etc may also connect to Access Switch.

Following diagram shows architecture for Data Capture locations.



Note: It is clarified that 18 DCCs are standalone, however 3 DCs are inter-connected.

Detailed Scope of Work

General

1. The SI shall supply all necessary Hardware, Software and licenses etc. as per "**Bill of Material"** / Work Order and in accordance with minimum specifications as provided in "**Bill of Material"**. Higher version /additional specifications shall be accepted.
2. All the supplied equipment & licenses should be in the name of the purchaser.
3. The SI shall be responsible for providing all equipment, software and services, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability and reliability of complete solution within the quoted/ contract price.

Virtualization Software (Hypervisor) & Manager

The System Integrator (SI) shall perform following work:

1. Configure single centralized manager to control and manage the virtual infrastructure as well as for real time monitoring of both physical and virtual components.
2. Configure Virtualization Management solution.
3. Integrate Virtualization Manager with Chassis and Blades.
4. Configure network bonding/ connectivity, VLANs, tunnel, etc wherever required and connectivity of all Blades with access switches.
5. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and virtual machine backup configuration.
6. Configure storage policies to provisioning of storage resources to ensure that each VM gets the specified storage resources and services.
7. SI shall perform integration of Storage with the proper backup solution and should enable integration with VM to perform backup of VM data and configuration files on VTL.

Network and Security Components

1. The SI shall arrange for Supply, Installation and commissioning of network & security components (including firewall, router, core & access switch, ADC, WAF, SIEM, End Point Protection, DLP etc.) as per "Bill of Material" in High Availability (HA) and should be configurable in Active-Active and Active-Passive mode at DC & DRC.
2. Setup of Core-Access Architecture with non-blocking uplinks between Core & Access Switches.
3. The support should be available 24x7x365 with unlimited updates during the complete tenure of the project without any additional cost, from the date of commissioning.
4. Configurations of network components from time to time as per requirement of purchaser.
5. Please note: **Security Equipment's i.e. Firewall, NIPS, Web Application Firewall, End Point Protection should be of different OEMs**

Disaster Recovery (DR)

The SI shall arrange for Supply & Installation of all the ordered items at two Disaster Recovery Sites (location mentioned in Data Sheet) or any other location (specified at a later stage) and submit the delivery challan of all the items mentioned in "**Bill of Material Section**" and **"Technical Specifications Section"** in the time-schedule mentioned at "Project Activity, Deliverables & Timelines" of this RFP.

The connectivity between DC, DRC-1 & DRC-2 site will be provisioned by purchaser.

The SI shall ensure that all hardware is supplied with all the required installation material/ accessories (wherever required) for proper installation at DR Site. The supplied items shall be housed in at DR Site or as specified during the time of installation.

The supplied software's (wherever applicable) should include appropriate number of genuine OEM perpetual licenses (as applicable as per OEM licensing policy).

Purchaser, upon receipt of delivery of all the ordered items as per prescribed time schedule, will inspect all the supplied items to validate them in compliance against with the work order.

After supply of items, SI-H shall arrange installation of all the supplied items including licensed software and respective hardware through certified engineers at designated installation location.

SI-H shall integrate DC & DRC sites in Active-Passive mode or Active-Active mode as instructed by purchaser.

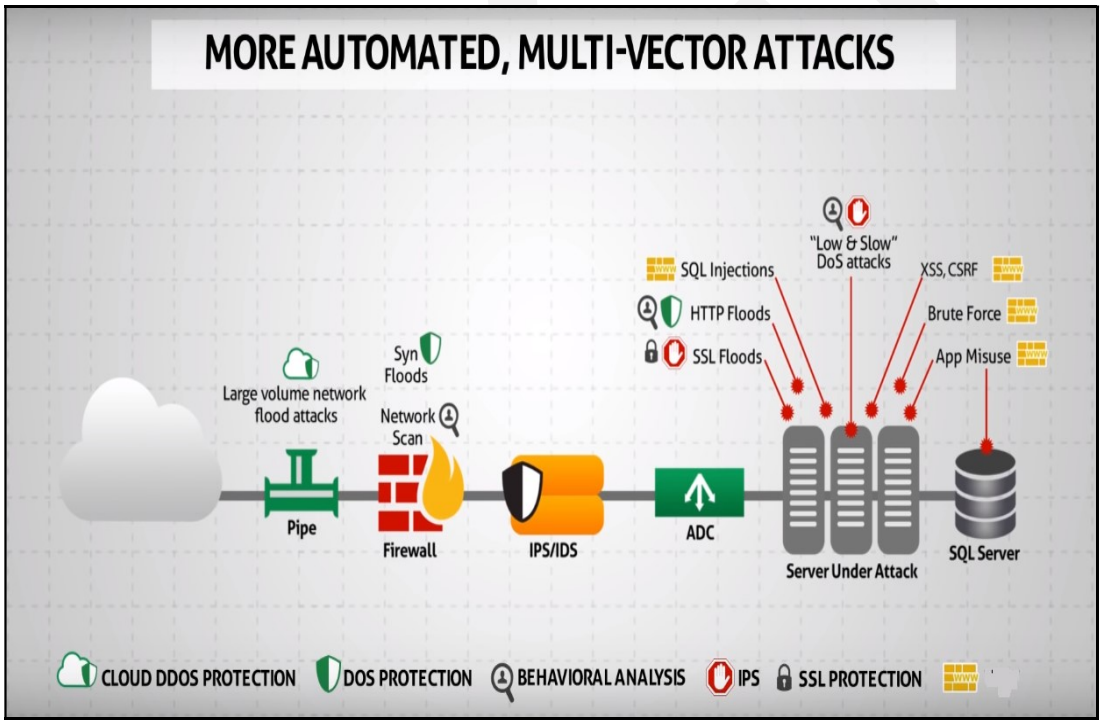
ORGI

Various components of Security solution should deliver results mentioned briefly in following section:

DDoS Protection Solution

Cyber-attacks have reached a tipping point in terms of quantity, length, complexity and targets. As cyber threats grow and expand to new targets, even organizations with by-the-book security programs can be caught off guard.

a) Attacks Are Longer, More Complex and Continuous.
b) Highly Motivated Attackers.
c) Network-Based Threats and Risks.
d) Application-Based Threats and Risks.
e) Zero-day Attacks.
f) Multi-Vector Attack.



DDoS Solution should use a dedicated hardware platform to prevent high volume DoS attacks and DDoS flood attacks, without impacting legitimate traffic. Blocking high packets-per-second (PPS) attacks that overuse the CPU resources of your networking and security equipment.

DDOS solution should provide attack Coverage with detection and mitigation of the following attack types:

1. Known and zero-day DoS/DDoS flood attacks that misuse network bandwidth resources.
2. Application DoS attacks that misuse server and application resources including:

a. HTTP/HTTPS and DNS flood attacks
b. SIP scans and flood attacks
c. Web stealth attacks (e.g., Login page brute force attacks, SSL-based attacks)

Detection and Mitigation

DDOS Solution should protect using Behavioral-based algorithms for attack detection that goes beyond just SYN flood protection to offer a wide range of protections at high mitigation capacity including SSL, DNS and more.

Unique messaging capability – that synchronizes attack information and baselines across the various elements of the solution to improve detection and mitigation response and accuracy.

Built with dedicated hardware platform to prevent high volume DoS attacks and DDoS flood attacks, without impacting legitimate traffic.

Automated Zero-Day DDoS Attack Protection

DDoS Solution should automatically generate DDoS prevention and protection for zero-day and unknown attacks. Within Few seconds, DDoS Solution should detect, characterize, and generate an optimal signature to block unknown attacks with a minimal false-positive rate.

Integrated Cyber Defense System

Offered Solution should have features which enables the different elements in Network solution to operate as a single system. This capability shall allow solution to apply the optimal detection technology deployment and maintain the ability to mitigate attackers at high performance and then push attackers to the perimeter of the network.

The solution should be designed to help organization's best attack mitigator by offering security solution that combines detection and mitigation tools.

Next Generation Network Firewall

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Network firewalls filter traffic between two or more networks and run on network hardware.

Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. They are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN server for that network. Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.

Packet Filters: Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set.

NAT: Firewall should have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range". Firewalls should have such functionality to hide the true address of computer which is connected to the network. NAT is considered a security feature, hiding the addresses of protected devices has become defense against network reconnaissance.

Access Control: Firewall should offer functionality to define access control to protected assets so that legitimate users get the application access and ill-legitimate traffic should be denied on Layer-3, Layer-4 and/or Layer-7 parameters. The firewall administrator may define the rules according to protected assets.

Stateful Inspection: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated, so that filtering decisions would not only be based on administrator-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection. To ensure faster application access, Appliance should offer 3 micro second or less latency to traffic passing through it.

Depending on the connection protocol, maintaining a connection's state is more or less complex for the firewall. For example, TCP is inherently a stateful protocol as connections are established with a three-way handshake ("SYN, SYN-ACK, ACK") and ended with a "FIN, FIN-ACK, ACK" exchange. This means that all packets with "SYN" in their header received by the firewall are interpreted to open new connections. If the service requested by the client is available on the server, it will respond with a "SYN-ACK" packet which the firewall will also track. Once the firewall receives the client's "ACK" response, it transfers the connection to the "ESTABLISHED" state as the connection has been authenticated bidirectionally. This allows tracking of future packets through the established connection. Simultaneously, the firewall drops all packets which are not associated with an existing connection recorded in its state table (or "SYN" packets), preventing unsolicited connections with the protected machine by black hat hacking.

Firewall should be IPV6 ready from day one with performance minimum 80 Gbps on IPv4 and IPv6 traffic.

VPN: VPN technology was developed to allow remote users and branch offices to access corporate applications and resources. To ensure security, the private network connection is established using an encrypted layered tunneling protocol and VPN users use authentication methods, including passwords or certificates, to gain access to the VPN. In other applications, Internet users may secure their transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. Firewalls come with SSL VPN feature, this helps roaming users to connect back and continue work in respective application hosted in data-center as and when they want. Roaming Users leverage mobile virtual private networks in settings where an endpoint of the VPN is not fixed to a single IP address, but instead roams across various networks such as data networks from cellular carriers or between multiple Wi-Fi access points without dropping or losing application sessions. Mobile VPNs are widely used in enterprise, where they give field users access to applications hosted in DC / DRC.

Virtualization: Firewalls are now available with virtualization option, means one physical firewall can be used as multiple virtual appliances in different segment of the network and hence helps in saving rack space, power, cooling and money.

Interfaces: Firewall should have sufficient 10G SFP+ interfaces along with option for 40G QSFP ports to ensure future safe investment.
Third party certification: OEM should have Firewall, IPSEC VPN and SSL VPN module certified by ICSA Labs. Offered product series should be EAL/ NDPP certified

Network Intrusion Prevention System

Network Intrusion Prevention System (NIPS) should fully protect the network infrastructure against known and emerging network security attacks.
NIPS should detect and mitigate following attack types:

- Application vulnerability attacks that exploit server application weaknesses including Web, Mail, DNS, FTP, SQL server vulnerabilities
- Server-based vulnerabilities:
    - Web-amplification vulnerabilities
    - Mail server vulnerabilities
    - FTP server vulnerabilities
    - SQL server vulnerabilities
    - DNS server vulnerabilities
    - SIP server vulnerabilities
- Worms and viruses
- Trojans and backdoors
- IRC bots
- Spyware
- Phishing

Dedicated Hardware to Fight Attacks

NIPS should use a dedicated hardware platform to prevent high volume intrusion attacks and flood attacks, without impacting legitimate traffic.

Multi-Segment Monitoring and Protection

NIPS will be deployed in transparent mode to monitor different segments in the network as shown in the Architecture diagram for DC and DR. All monitored segments will be 10GbE on SR optical. Protection policy for each segment will be defined as per the resource to be protected in that segment.

Security Patch Update

Security Patch Update is regular security advisory from OEM to update monitoring and detection service for enterprise network security. This will help to protect applications, network and users against the latest network and application security threats and recent denial of service attacks by delivering immediate and ongoing signature updates for worms, Trojans, BOTs, malware and various application vulnerabilities

Application Delivery Controller

Should deliver a holistic solution for SLA assurance and addresses the most current challenges and trends. SLB should innovatively leverages several next generation services, bundling Web Performance Optimization and Acceleration, Application

Performance Monitoring, Authentication Gateway, Application level Denial of Service, Bandwidth Management as well as maximum SSL and compression capacities.

Increased efficiency for server utilization and network bandwidth

Server Load Balancer should aware of the shared services provided by server pool and can then balance user session traffic among the available servers. Important session traffic gets through more easily, reducing user competition for connections on overused servers. For even greater control, traffic should be distributed according to a variety of user-selectable rules.

Increased reliability of services to users

If any server in a server pool fails, the remaining servers continue to provide access to vital applications and data. The failed server can be brought back up without interrupting access to services.

Layer 7 Capabilities

Taking action on the basis of Layer-7 header parameters will help when application changes are needed on the fly and reprogramming of the application is not possible, ADC's are the preferred choice to resolve the problem without interrupting the availability of the application servers.

Application Level Traffic Steering

When traffic needs to be directed to a specific server based on its functionality, Server Load Balancer can inspect application level request data (L7), classify the traffic, and perform the forwarding decision accordingly.

SSL Offloading

Server Load Balancer should utilize a unique software architecture which enables flexible allocation of CPU processing cores per function, such as SSL offloading. As a result, Server Load Balancer enables cost effective SSL offloading from the application servers it manages.

Global Load Balancing

Global Server Load Balancer should provide Geo-graphic load balancing and DC level redundancy by leveraging DNS. Solution should provide following features:

1. Geo-location based traffic routing to monitor availability and performance of global resources to manage the application load pattern.
2. Secure Global Application delivery with built-in protocol validation which automatically drop UDP DNS query flood and NX domain floods.
3. GSLB Solution should have capability of IP anycast to distribute the DNS request load by directing single IP request to multiple datacenters.
4. **DNS and DNS security (DNS & DNS Firewall) –** DNS based redirection will be used to achieve global load balancing between DC and DRC. GSLB appliance will be configured as full DNS server hosting various types of DNS records including A record, AAA record, PTR, MX, CNAME, SOA, SRV, TXT records. DNS solution for hosting authoritative DNS, resolver and Cache DNS with DNS security to protect the DNS infrastructure

Web Application Firewall

Web Application Firewall (WAF), ensures fast, reliable and secure delivery of mission-critical Web applications. WAF Should be an ICSA Labs certified and PCI compliant WAF that provides complete protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages.

Solution should protect from Mobile application based attacks through antibot mobile SDK.

Protection from Zero-Day Web Attacks

Should Use both negative (signature based) and positive security models. Web application firewall (WAF) features not only the lowest false positives and minimal operational effort, but also robust protection against known and unknown (Zero-day) threats. WAF Solution should protect from browser based malware, which can steal sensitive information like username/ password, OTP etc without any additional client-side agent.

Full Coverage of OWASP Top-10 Out-of-the-box

Including injections, cross-site scripting (XSS), cross-site request forgery (CSRF), broken authentication and session management and security misconfiguration. Identifying and blocking sensitive information transmission such as credit card numbers, Social Security number, Aadhaar number.

Device Fingerprinting for Advance Bot Protection

WAF Should be agnostic web-application security solution. It should disregards IP source address context to protect from dynamic IP attacks. The power of the fingerprint is in the consolidated information extracted from dozens of browser attributes collected on the client side, facilitating accurate bot classification. Solution should detect and mitigate bot traffic by using challenge response mechanism escalating JavaScript and CAPTCHA challenges/ Device Finger Printing.

Leveraging Machine-Learning Algorithms for Auto Policy Generation

WAF should incorporates machine-learning algorithms to keep Web assets protected always, even while applications constantly change and threats rapidly evolve, assuring web security is future proof. WAF's should have unique ML powered Auto Policy Generation mechanism providing the best tool for automatically generating security policy for the secured Web application.

The Auto Policy Generation module will automatically utilize the required security filter, create security filter rules and switch the security filters into active mode.

Leveraging machine-learning algorithms, Auto Policy Generation should secure web application as automatically as possible with minimal user interaction. This should get following benefits:

- Shortest time to protection
- Performing auto threat analysis with no admin intervention
- Lowest false-positives through auto-optimization of out-of-the-box rules
- Automatic detection of web application changes assuring security throughout the application's development lifecycle – **post deployment peace of mind**

<u>Situational Awareness & Security Analytics</u>

Every connected asset on the network is a potential target. It has been globally recognized that it takes an attacker a few minutes to a few hours to inflict a breach but, it takes over 100 days for an organization to detect the attack. Abetting this issue for those responsible for an organization's cyber security are diminishing perimeter and widening scope of "usable" tools – that are no longer limited to workplace data-centre technologies but applications in the public domain to which traditional IT or Security have no control or visibility.

Consequentially, security experts recognize the need to have a comprehensive visibility of network environment using Deep Packet and Payload Inspection technology that allows ability to profile device and application activities in real-time and, enables knowledge-based detection of malicious activities, Denial of Service Attacks, internal reconnaissance attempts and, other suspicious activities. Given that presence of unknown actors/techniques cannot be overlooked, the solution should leverage field tuneable Machine Learning algorithms and heuristics to detect anomalous activities without actually impacting any network or uptime SLA's.

As the network expands, the solution should not be just limited to a single-instance/single-appliance but scale out to support an array of DPI sensors with a comprehensive multi-sensor management, monitoring and analytics framework. For applications such as SSH, SSL/TLS, IPSec and others that use ciphers – traditional or custom, the solution should be able to analyse such communication and provide meaningful insights that may be helpful for risk or performance management without using any man-in-the-middle network or application layer gateways.

ORGI

DataBase Activity Monitoring (DAM) and Firewall

Data is the lifeblood of today's organizations. Any interruption, unintended disclosure, or loss of data could spell disaster. Even though databases often contain organization's most important information, they tend to be the least protected. In our case it will be information about citizens and demographic detail. As per some researches, more than 90 percent of records breached involve a database. And up to 50% of those breaches are attributed to internal users.

Despite the fact that vendors regularly issue security updates, many organizations often delay installing them, or simply do not install them at all. While this hesitancy to install patches is understandable and stems from a variety of reasons, it creates a dangerous situation for the organizations because it introduces a "window of vulnerability"—the period of time between the issuance of a vendor security patch and the installation of the patch.

Within days (or hours, in some cases) of a vendor patch release, the social network of black hats is rife with details on the nature of the underlying problem and how to leverage it to penetrate database servers that have not yet been patched. Of course, a few sophisticated hackers also discover their own zero-day vulnerabilities.

The net result is that a compromised database could allow an attacker to deny availability to legitimate users, inject malicious content, or access sensitive information. In some cases, changes can be made to the database structure itself, even to the extent of dropping tables entirely.

By monitoring all activity occurring in the database memory and detecting "fingerprints" of known exploits and vulnerabilities, virtual patching identifies attempted attacks. When a match occurs, an alert is issued in real time, the suspicious session can be terminated, and the originating user can be quarantined for a specified period until the nature of the suspected attack is investigated.

Database Activity Monitoring should automatically find databases on network, protects them with a set of preconfigured defences, and helps build a custom security policy for environment — making it easier to demonstrate compliance to auditors and improve critical asset data protection. Database Activity Monitoring cost-effectively protects data from all threats by monitoring activity locally on each database server and by alerting or terminating malicious behavior in real time, even when running in virtualized or cloud computing environments.

A single Management server can manage and communicate with numerous sensors on different databases, and an enterprise installation can easily scale up to encompass hundreds of databases. The server also easily integrates with IT infrastructure to facilitate central IT management and security event management.

Since the sensor is installed on the database machine, it is impossible to bypass and possesses self-defense mechanisms that alert on any tampering attempts. The structure of the system also

ensures separation of duties, a key requirement in IT security. The administrator, the person defining policy rules and the person receiving alerts can all be different people in different departments within the organization.

Database Activity Monitoring solution should perform following:
1. Database Activity Monitoring Solution should maximize visibility and protection from all sources of attacks on database servers.
2. Offered solution should be implemented with Centralized monitoring, in HA, for databases across datacenters.
3. Provide post-sales supports from support center in India.
4. It should be an Agent based solution and should not require a network appliance for scanning database traffic.
5. Single agent based solution for database firewall, database vulnerability management, database access management and virtual patching.
6. Offered solution should monitor external threats, privileged insiders, and sophisticated threats from within the database.
7. Offered solution should minimize risk and liability by stopping attacks before they cause damage.
8. Offered solution should quickly builds a custom security policy to meet industry regulations or internal IT governance standards.
9. Offered solution should log access to sensitive data for audit purposes, including complete transaction details.
10. Offered solution should locate and identify tables containing sensitive information across databases.
11. Offered solution should conduct a quick port scan providing database version and patch status.

Patch Management Solution

Robust patch management is need of the day for today's threats Patching servers often requires longer implementation cycles due to the necessary demands of pre-testing to minimize potential service disruptions. Both IT operations and security are forced into a dilemma of leaving servers exposed or installing potentially disruptive patches. Server Management Suite improves overall security by providing automated, robust patch management for multiple server operating systems including all Microsoft and Linux updates. Patch management solution should support for security and non-security related updates along with commonly used third-party applications.

Automation

Patch Management Solution should offer capability to automate the remediation of vulnerabilities. Solution should scan for vulnerabilities in our environment and the results should be used to kicks off the delivery of patches to the endpoints that need to be remediated. Solution should automate the delivery of these patches if desired such as those considered critical or high risk.

Offered solution should allow ORGI to define, design and deliver automated IT processes and workflows that drive business. The software delivers improved automation of day to day or redundant client systems management tasks. End to end automation should be done using operational, productivity, and event-based decision rules. Workflow simplifies process creation and modification with a visual, drag-and-drop design interface that doesn't require coding. Process automation helps to bring people, process, and systems management together using a single tool.

Solution should cater to wide environment conditions and challenges, such as remote isolated areas with high network latency and low bandwidth connections. No dependency on Active Directory also eliminate any unnecessary network bandwidth utilization from Active Directory data replication.

The solution should cover complete patch management for Linux, including automated patch bulletin feeds with severity information and binary packages. The solution should have Peer-2-Peer distribution of patch and software packages with rich bandwidth control and management capability and should recognize and control actual bandwidth at each endpoint. The solution must be capable to download and cache payload at the remote distribution points before the scheduled time of an action. This will ensure timely completion of activities within scheduled window without having to wait for downloads to complete during scheduled window over slower WAN links. This reduces the vulnerability window form any cyber-attack events. At the same time resulting in much less number of distribution servers reducing the attack surface from any cyber-attack activities.

The solution should have full feature and integrated asset management capability for complete endpoint lifecycle management. Include capability such as software license management, to achieve license compliance and savings from better license consumption. The solution must support users connecting through VPN and internet connected users. Any additional software /hardware to support such remote users should be included in the solution proposed.

Effective remediation of vulnerabilities: Along with wide range of operating system; solution should support for the largest number of 3rd party non-Microsoft application patch and updates. This should include update and patch bulletins feeds from the software vendors, corresponding to the downloadable version of the software to be deployed to the endpoint.

Effective Protection Against Vulnerabilities

Centralized and simplified patch management, supporting broad operating systems from Windows, Mac OS X, Linux and Unix. Including broad support across applications; extending beyond Microsoft application, to include over 50 third party applications.
Client Management Suite should offer network adaptability for low bandwidth needs. It should provide static and dynamic bandwidth throttling capability, automatically adjusting itself to the available network bandwidth. Offered solution be effective and efficient in managing network bandwidth hence ensuring less network bandwidth consumed and no impact on core business applications, and eventually no business impact.

Captive Security Operation Centre (SOC)

Every connected asset on the network is a potential target. It has been globally recognized that it takes an attacker a few minutes to a few hours to inflict a breach but, it takes over 100 days for an organization to detect the attack. Abetting this issue for those responsible for an organization's cyber security are diminishing perimeter and widening scope of "usable" tools – that are no longer limited to workplace data-centre technologies but applications in the public domain to which traditional IT or Security have no control or visibility.

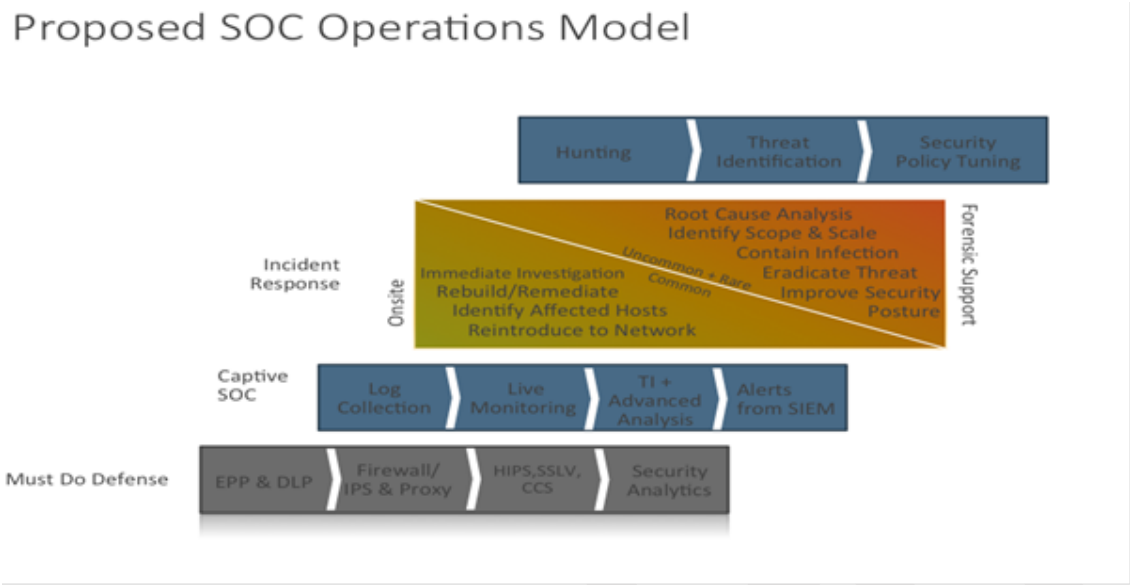
Consequentially, security experts recognize the need to have a comprehensive visibility of network environment using Collection and correlation of all security logs generated byy all security components in the network along with Deep Packet and Payload Inspection technology that allows ability to profile device and application activities in real-time and, enables knowledge-based detection of malicious activities, Denial of Service Attacks, internal reconnaissance attempts and, other suspicious activities. Given that presence of unknown actors/techniques cannot be overlooked, the solution should leverage field tuneable Machine Learning algorithms and heuristics to detect anomalous activities without actually impacting any network or uptime SLA's.

As the network expands, the solution should not be just limited to a single-instance/single-appliance but scale out to support an array of DPI sensors with a comprehensive multi-sensor management, monitoring and analytics framework. For applications such as SSH, SSL/TLS, IPSec and others that use ciphers – traditional or custom, the solution should be able to analyse such communication and provide meaningful insights that may be helpful for risk or performance management without using any man-in-the-middle network or application layer gateways.

ORGI wants to set-up state-of-art scalable SOC to reduce the time between detection and response, and minimize the business impact of any cyber attack with continual advanced security monitoring. In this evolving cyber landscape, attackers move faster, threat actors are smarter, and the time to detect an attack is also increasing. Thus, ORGI wants SOC operation to be set-up including expertly monitoring environment for 24x7 monitoring with on-site resource expertise, global security OEM advance incident response service and global security OEM threat intelligence to detect advanced attacks. The OEM being considered for such services should be a leader in managed security services for at least five years and should have been providing such threat intelligence for at least 10 years. The MSI should complement the SOC operation with the security infrastructure as proposed in RFP to improve the security operations program and better manage the ORGI's security posture before, during, and after an attack.

Security Operation Centre Operation Model

Following diagram describe the high-level operation model for SOC. SI to design as per the function required and scope of work as given in the RFP.



SOC Scope of Work:

Based on the requirements of ORGI following is the minimum Scope of work to be considered by MSI:

1. Security Incident & Event Management (SIEM) Optimization and SOC Governance and Process Development

- SIEM Technology Optimization – Validate and optimize the SIEM deployed in the ORGI environment for
  - *SIEM*
    - Review the SIEM Architecture for scalability (Handling events and EPS), Redundancy (DR and switch over) and Compliance with Licenses.
    - Review the existing events and alerts to identify false positives, non-actionable rules and partial rule matches
    - Review the existing SIEM rule bases for appropriate correlation conditions
    - Review the coverage of Log sources/ data sources.
    - Create a minimum of 10 additional use cases aligned with kill chain model of threat mitigation.
    - Fine tune existing use cases to reduce false positive
  - *Security Intelligence*
    - Verify if the existing sources for threat intelligence information is identified, subscribed and is acted upon.
    - Verify if the external threat intelligence feeds are automated.
  - *Incident Management Platform*
    - Identify the availability of the ticketing system, the information captured in the incident, its automation via API integration and escalation via workflows and develop as required.

    - Review the maturity of incident response via technology integration to search and apply responses, collaboration and escalation, learning and feedback for SIEM enhancement.
    - Integration with ISIRT/ CERT teams.
- Governance – Verify and create governance framework to identify the SOC organization, roles and responsibilities of SOC organization, integration with business, IT and CERT and business and compliance reporting, improvement and metrics. It is expected from the SP to create the documents with a minimum of 5 customized reports and 2 weekly and monthly analyst reporting. It is expected to define minimum of 10 metrics to measure the effectiveness of SIEM, Use cases (SIEM rules) and incidents and alerts (false positive, true positive, MTTD etc.)
- Processes - Define a set of processes for Monitoring and Notification, Triage and Escalation, Incident Response recommendations based on Use Cases, device on-boarding procedure, threat intelligence and actionable process and SLA reporting and measurement.

ORGI

Annexure – C1: List Of Hardware/ Networking Equipment at 18 DCC locations

S. No.	Data Centre Location	42 U Rack	Server Type-2 (2*16Core CPU and 512GB RAM) along with enclosure	MS Windows Server STD edition (Latest version) with 16 core license	Internal / External Storage in RAID6 (in TBs) with 20%on SSD and 80% on 10K SAS)	Workstation	Multifunction printer (Mono)	Mono Laser Printer	Core switch Type-2	Access Switch	Capacity of On-Line Modular UPS in KVA	Anti Virus for servers and workstations
1	2	3	4	5	6	9	10	11	12	13	14	15
1	Bengaluru	0	3	6	75	91	1	2	1	4	60	101
2	Bhopal	1	3	6	75	111	1	2	1	5	60	114
3	Bhubaneswar	1	3	6	75	63	1	2	1	3	40	66
4	Chandigarh	1	3	6	75	106	1	2	1	3	60	109
5	Chennai	1	3	6	75	118	1	2	1	3	80	121
6	Delhi RKP	1	3	6	75	118	1	2	1	3	60	121
7	Gandhinagar	1	3	6	75	84	1	2	1	3	60	87
8	Guwahati	1	2	4	50	81	1	2	1	2	40	83
9	Hyderabad	1	4	8	100	133	1	3	1	3	80	137
10	Jaipur	1	3	6	75	96	1	2	1	3	60	99
11	Kolkata	1	4	8	100	133	1	3	1	4	80	137
12	Lucknow	0	4	8	100	128	1	3	1	4	80	139
13	Mumbai	1	4	8	100	154	1	3	1	4	80	158
14	Patna	1	4	8	100	141	1	3	1	4	80	145
15	Thiruvananthapuram	1	2	4	50	60	1	1	1	2	40	62
16	Ranchi	1	2	4	50	47	1	1	1	2	40	49
17	Raipur	1	2	4	50	43	1	1	1	2	40	45
18	Dehradun	1	2	4	50	66	1	2	1	2	40	68
19	NDC, Delhi	0	0	0	0	68	1	2	0	10	**0**	125
	Total	**16**	**54**	**108**		**1841**	**18**	**38**	**18**	**66**		**1966**

Annexure – C2: Components at 3 Data Centers

Type & Quantity of Components to be installed at three Data Centers to ensure smooth transmission of Data from Mobile/ Web Application to Central Servers

S.No.	Components	Data Centre Location		
		NDC, ORGI	Bengaluru	Lucknow
1	Smart Rack	0	1	1
2	Blade Server Type-1 (4*20Core CPU and 2TB RAM) with enclosure	7	7	7
3	SAN Switch	4	2	2
4	Core switch Type-1	2	2	2
5	External Storage Usable Capacity in RAID6 (in TBs) with 20%on SSD and 80% on 10K SAS)	1,000	1,000	1,000
6	Virtual Tape Library Capacity in TBs with 20% of Internal External Storage Capacity	200	200	200
7	Back-up Software (License for TB)	80	80	80
8	Distributed Denial of Service (DDOS) Protection	2	2	2
9	Firewall with Virtualization	2	2	2
10	Network Intrusion Prevention System (NIPS)	2	2	2
11	Application Delivery Controller with GSLB	2	2	2
12	Web Application Firewall	2	2	2
13	Network Access Control (NAC) Authorised Hosts	200	25	25
14	Data-Base Activity Monitoring (DAM)	5	5	5
15	Patch Management	200	25	25
16	Host based Intrusion Prevention System for Servers	50	25	25
17	Endpoint Protection and Remediation	200	25	25
18	Data Leak Prevention (Client based DLP)	200	25	25
19	Setting up of Captive Security Operation Centre (SOC) including SIEM, Threat Feed, Incident Response Service and Man-Power	1	0	0
20	SIEM Log Collector	1	1	1
21	Situational Awareness & Analytics	1	1	1
22	MS Windows Server STD edition (Latest version) for 7 Nos. 80 Cores Servers.	35	35	35
23	Visual Studio Enterprise (latest version)	1	1	1
24	Router for Internet	4	4	4
25	MFP Colour Printer	1	0	0
26	Link Load Balancer	2	2	2
27	Virtualisation Software: Nos. of Servers required to be virtualised (Minimum 10 virtual machines on each Server)	3	3	3

Annexure – C3: List & Quantity of Software to be installed

Sr. No.	DCC Center	Number of MS Office Professional Latest Version	Number of MY SQL Enterprise Server Latest Version
1	Bengaluru	2	2
2	Bhopal	2	1
3	Bhubaneswar	2	1
4	Chandigarh	2	1
5	Chennai	2	1
6	Delhi	3	1
7	Gandhi Nagar	2	1
8	Guwahati	2	1
9	Hyderabad	2	1
10	Jaipur	2	1
11	Kolkata	2	1
12	Lucknow	3	2
13	Mumbai	3	1
14	Patna	2	1
15	Trivandrum	2	1
16	Ranchi	2	1
17	Raipur	2	1
18	Dehradun	2	1
19	NDC, ORGI	2	2
	Total no. Quantity	**41**	**22**

Annexure – C4: Link Load Balancer for 3 Data Centres

S.No.	Specifications
1	Throughput - Minimum 40 Gbps
2	The proposed device should be a dedicated purpose built hardware Load Balancer appliance. It should not be a part of UTM, Firewall module or Router functionality.
3	Platform should be a full proxy architecture and must perform reverse proxy for inside applications.
4	Should have a dedicated out-of-band Ethernet management port
5	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
d	DNS on IPv6 to IPv4 and vice versa
6	Should support VLAN, LACP & Trunking
7	Should have a SSD HDD with minimal capacity of 400 GB
8	Should have 4 x 1 Gigabit SFP Sx Ports, 4x10Gig SFP+ SR and minimum 4x40G QSFP+ SR ports, fully populated
9	Should have dual power supply
10	Proposes solution should have system throughput of 40Gbps and scalable upto 60Gbps
11	Should have capability to support up to 40 Million Concurrent Connections
12	Should support configurable TCP Optimization features for client-side and server-side connection
13	Should support for minimum 10 ISP links
14	The Solution should be able to perform inbound load balancing using DNS. DNS service should have capability individual record type including: A, AAAA, Any, AXFR, CNAME, IXFR, MX, NS, PTR, NS, SOA, SRV, TXT.
15	Selection of shortest path to Destination based on load, Hops, Response time
16	Should support static & dynamic based outbound as well as inbound load balancing
17	Should support load balancing algorithms
a	Least amount of Bytes
b	Least number of users/session.
c	Cyclic, Weighted Cyclic.
d	Ratio Based
e	Healthy Link Priority to use the healthy link in case of fluctuation in link
18	Should support Static NAT & Dynamic NAT with NAT64
19	Device should detect link failure within 20 seconds and divert the traffic to other available links.
20	Should support Bandwidth management on multiple links.
21	Link Load balancer should support dynamic routing protocol like BGP, OSPF and RIP
22	The proposed solution must support Bandwidth Management for multiple links on Layer-3 to Layer-7 parameters.
23	Should provide HTTPS, SSH interface management for administering the device

24	Should have a live dashboard with graphical reporting
a	CPU Usage
b	Memory Usage
c	Connections Statistics
d	Throughput Statistics
e	Virtual Server Status
f	Real Server Group/ Pool Status
g	Node Status
25	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL Connection mirroring. Hence old connection should not fail or forced for SSL renegotiation.
26	Should have transparent failover between 2 devices, the failover should be transparent to other networking devices
27	Should support network based failover for session mirroring, connection mirroring and heartbeat check
28	Should support config autosync, manual sync to and from active and backup unit
29	Should have a Reporting Engine built-in
30	Solution should provide the application visibility and hostorical reporting with below metrics and entity for each application:
a	Client IP addresses / subnets as well as geographical regions
b	Total Transactions as well as Average and Max Transactions/sec
c	Most commonly requested URLs
d	Server Latency and Page Load times
e	Page Load Time
f	Response code
g	OS and Browser
h	URL details
31	Proposed solution should be EAL/ NDPP or ICSA Certified

Annexure – C5(a): Server with Enclosure Type 1 for 3 Main Data Centres

(i) Specifications for Server (4*20 Core CPU and 2TB RAM) for 3 Nos. Main Data Centres at Delhi, Bengaluru & Lucknow

Item	Specifications
CPU	Each blade shall have four numbers of latest Intel Xeon Scalable Processors with Minimum Twenty cores per processor each having Minimum 2.5 GHz processor speed.
Motherboard	Intel C621 Series Chipset
Memory	2.0 TB Memory scalable up-to 4.0 TB using DDR4 memory operating at 2933 MT/s.
Memory Protection	Advanced ECC with multi-bit error protection.
Hard disk drive with carrier	Minimum 2 x 3.84 TB hot plug SAS 12G SFF SSD.
Storage Controller	Integrated or Addon 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5
Networking features	Converged Network Adaptor with minimum 40Gbps bandwidth
Operating System	Red Hat Linux Enterprise (Latest Version).
Bus Slots	Minimum of 3 Nos of PCIe 3.0 based mezzanine slots supporting Converged / Ethernet/ FC adapters.
Industry Standard Compliance	Microsoft® Logo certifications
	WOL (Wake On LAN) /Auto Discovery enabled on specific adapters with Blade solution
	PXE support enabled
	USB 3.0 Compliant
	TPM 2.0 Support (RBSU support for TPM 1.2)
	IEEE (specific IEEE standards depending on Ethernet adapter card(s) installed) /FCoE based solution
	Advanced Encryption Standard (AES)
	Triple Data Encryption Standard (3DES)
	SNMP
	Latest version of SSL / TLS
	Latest version of Active Directory
	Latest Version of PCIe Compliant
	UEFI (Unified Extensible Firmware Interface Forum)
OS Support (Latest Version)	Microsoft Windows Server
	Red Hat Enterprise Linux (RHEL), Ubuntu
	SUSE Linux Enterprise Server (SLES)
	Virtualization
Embedded Remote Management and firmware security	System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication.
	Server should have dedicated remote management or remote management functionality.
	Server should support agentless management using the out-of-band remote management port.

	Remote console sharing simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.
	Should support RESTful/XML API integration..
	System should support embedded remote support with consent of ORGI to transmit hardware events directly to OEM or an authorized partner for automated phone home support.
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.
	The Dashboard minimum should display a health summary of Server Profiles, Server Hardware, Appliance alerts
	The Systems Management software should provide Role-based access control
	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
	The Server Management Software should be of the same brand as of the server supplier.

ORGI

(ii) Specifications for Enclosure for 3 Nos. Main Data Centres

Item	Specifications
Solution requirement	Proposed solution should support provisioning infrastructure from pools of compute, storage and networking resources
	Proposed solution should be able to manage and monitor both existing and new infrastructure from the single management GUI. All necessary software licenses required needs to be included.
	Solution should have single console provisioning for compute, storage and server side network configuration.
	Solution should support API to integrate into popular management tools such as Microsoft System Center and VMW are vCenter and into open source automation and DevOps tools such as Chef, Docker and OpenStack.
	Solution should support software defined templates to quickly make changes to the infrastructure.
Blade Chassis	Solution to house the required number of blade servers in smallest number of enclosures. Should support half height/single width and full height / double width blades in the same enclosure. Should support minimum 8 number of 2 CPU servers or 4 number of 4 CPU servers
	Should support redundant interconnect bays to configure
	Should support built-in/external management software appliance in redundancy with separate management network from production network
	Should support technology built-in to every chassis for Auto-Discovery of resources
	Should support linking multiple enclosures together to form single management ring or managed through a central management platform, to reduce complexity and provide single console of management for connected enclosures.
Interconnects support	Should support housing of FCoE, Ethernet, FC and SAS interconnect fabrics offering redundancy as a feature.
Converged Interconnect	Interconnects should support minimum 40Gbps downlinks bandwidth to each Blade Server.
	Redundant Interconnect modules shall be integrated within the chassis such that uplinks from the chassis can be directly connected to core LAN/SAN switches.
	Should support aggregation of multiple enclosures to consolidate data center network connections, reduce hardware and to scale network bandwidth across multiple enclosures. Minimum 36 servers should be supported per aggregation. Layer 2 network traffic should be switched within enclosure aggregation (without using top of the rack switch)
	Aggregation Switch/modules must be offered with at least 80Gbps for external uplink connectivity for Ethernet LAN to Core Switch and 64Gbps bandwidth for FC uplinks to the SAN Fabric. All the modules/ switches for chassis interconnectivity should be in redundancy with 1:1 connectivity.
Power Supply	1. The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should be supplied with N+N.
Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics

System Software	Management/controlling software have to be from the hardware OEM.
Management capabilities	Solution should support redundant physical management appliances within/ outside the enclosure with failover and high-availability
	Should support auto-discovery of Compute, Memory, Storage and Fabrics within an enclosure or on multiple connected enclosures.
	Should support activity, Health and Power LEDs/LCD for immediate status
	Should support software-defined intelligence for configuring profiles to provision compute, storage, fabrics and images
	Should support Firmware and OS Driver updates for the servers using profile templates to monitor, flag, and remediate
	Should provide a dedicated 1GbE or higher management network for multi-enclosure communications, separate from data plane
	Should support reporting capabilities for:
	1) Asset and inventory information for the devices in the enclosures
	2) Thermal and power information, including real-time actual power usage per server and per enclosure.
Integration with virtualization and open source software	Should support integration with popular virtualization offerings VMware v Center and Microsoft system center
	Should support integration with open source automation and DevOps tools such as Chef, Docker, and OpenStack

Annexure – C5(b): Server with Enclosure Type 2 for 18 Data Capture Centers

(i) Specifications for Server (2*16 Core CPU and 512 GB RAM) for 18 Nos. Data Capture Centres

Item	Specifications
CPU	Each blade shall have two numbers of latest Intel Xeon Scalable Processors with Minimum 16 cores per processor each having Minimum 2.8 GHz processor speed.
Motherboard	Intel C621 Series Chipset
Memory	512 GB Memory scalable upto 2.0 TB using DDR4 memory operating at 2933 MT/s.
Memory Protection	Advanced ECC with multi-bit error protection.
Hard disk drive with carrier	Minimum 2 * 3.8 TB hot plug SAS 12G SFF SSD.
Storage Controller	Integrated or Addon 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5
Networking features	Converged Network Adaptor with minimum 40Gbps bandwidth
Bus Slots	Minimum of 3 Nos of PCIe 3.0 based mezzanine slots supporting Converged / Ethernet/ FC adapters.
Industry Standard Compliance	Microsoft® Logo certifications
	WOL (Wake On LAN) /Auto Discovery enabled on specific LAN adapters with Blade solution
	PXE support enabled
	USB 3.0 Compliant
	TPM 2.0 Support (RBSU support for TPM 1.2)
	IEEE (specific IEEE standards depending on Ethernet adapter card(s) installed) /FCoE based solution
	Advanced Encryption Standard (AES)
	Triple Data Encryption Standard (3DES)
	SNMP
	Latest Version of SSL/ TLS
	Latest Version of Active Directory
	Latest Version of PCIe Compliant
	UEFI (Unified Extensible Firmware Interface Forum)
OS Support (Latest Version)	Microsoft Windows Server
	Red Hat Enterprise Linux (RHEL), Ubuntu
	SUSE Linux Enterprise Server (SLES)
	Virtualization
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication
	2. Server should have dedicated remote management.
	3. Server should support agentless management using the out-of-band remote management port.

	4. Remote console sharing simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.
	5. Should support RESTful/XML API integration
	6. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.
	The Dashboard minimum should display a health summary of Server Profiles, Server Hardware, Appliance alerts
	The Systems Management software should provide Role-based access control
	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
	The Server Management Software should be of the same brand as of the server supplier.

(ii) Specifications for Enclosure for 18 Nos. Data Capture Centres

Item	Specifications
Solution requirement	Proposed solution should support provisioning infrastructure from pools of compute, storage and networking resources
	Proposed solution should be able to manage and monitor both existing and new infrastructure from the single management GUI. All necessary software licenses required needs to be included.
	Solution should have single console provisioning for compute, storage and server side network configuration.
	Solution should support API to integrate into popular management tools such as Microsoft System Center and VMWare vCenter and into open source automation and DevOps tools such as Chef, Docker and OpenStack.
	Solution should support software defined templates to quickly make changes to the infrastructure.
Blade Chassis	Solution to house the required number of blade servers in smallest number of enclosures.
	Should support half height/single width and full height / double width blades in the same enclosure.
	Should support minimum 8 number of 2 CPU servers or 4 number of 4 CPU servers.
	Enclosure should be offered with storage blade within enclosure along with a compute module to configure as DAS. Total usable _____ TB capacity (as per the ANNEXURE- C1 List of Hardware & Networking Equipment) Offered in 20% SSD with Raid-5 and 80% 10K SAS with RAID-6. In case bidder wants to offer external storage, the same can be offered with the capacity mentioned, for technical specifications refer Annexure - C13 (c).
	Should support redundant interconnect bays to configure
	Should support built-in/external management software appliance in redundancy with separate management network from production network
	Should support technology built-in to every chassis for Auto-Discovery of resources
	Should support linking multiple enclosures together to form single management ring to reduce complexity and provide single console of management for connected enclosures
Interconnects support	Should support housing of FCoE, Ethernet, FC and SAS interconnect fabrics offering redundancy as a feature.
Converged Interconnect	Interconnects should support minimum 40Gbps downlinks bandwidth to each Blade Server.
	Redundant Interconnect modules shall be integrated within the chassis such that uplinks from the chassis can be directly connected to core LAN/SAN switches.
	Should support aggregation of multiple enclosures to consolidate data center network connections, reduce hardware and to scale network bandwidth across multiple enclosures. Atleast 36 servers should be supported per aggregation. Layer 2 network traffic should be switched within enclosure aggregation (without using top of the rack switch)

	Aggregation Switch/modules must be offered with at least 80Gbps for external uplink connectivity for Ethernet LAN to Core Switch and 64Gbps bandwidth for FC uplinks to the SAN Fabric. All the modules/switches for chassis interconnectivity should be in redundancy with 1:1 connectivity.
Power Supply	1. The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should be supplied with N+N.
Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics
System Software	Management/ controlling software have to be from the hardware OEM.
Management capabilities	Solution should support redundant physical management appliances within/ outside the enclosure with failover and high-availability
	Should support auto-discovery of Compute, Memory, Storage and Fabrics within an enclosure or on multiple connected enclosures.
	Should support activity, Health and Power LEDs/LCD for immediate status
	Should support software-defined intelligence for configuring profiles to provision compute, storage, fabrics and images
	Should support Firmware and OS Driver updates for the servers using profile templates to monitor, flag, and remediate
	Should provide a dedicated 1GbE or higher management network for multi-enclosure communications, separate from data plane
	Should support reporting capabilities for
	1) asset and inventory information for the devices in the enclosures
	2) thermal and power information, including real-time actual power usage per server and per enclosure
Integration with virtualization and open source software	Should support integration with popular virtualization offerings VMware vCenter and Microsoft system center
	Should support integration with open source automation and DevOps tools such as Chef, Docker, and OpenStack

Annexure – C6: Workstation

Features	Specifications
Processor	Intel® Xeon® E-2224G 3.5Ghz, 8MB Cache, 4 Core or better for 24x7 operation
Chipset	Intel® C246 chipset
RAM	16GB Memory & speed should be 2666 MHz or better
	4 DIMM slots, supporting up to 64GB ECC/non-ECC, DDR4 2666 MT/s
Drive Controllers	Integrated SATA controller with minimum 4 x 6Gbps ports Support for RAID 0,1
HDD	1TB 7200 RPM SATA Drive or higher
Graphics Card	Dedicated 2 GB Professional Series Graphic card or higher.
Keyboard and Mouse	Mechanical Keyboard and USB Optical Scroll mouse. Third party Keyboard is acceptable.
Audio	High Definition Integrated Audio with Internal speaker
Communications	Integrated Intel® I219LM GbE Controller with Intel® vPro™ with Intel® AMT 12.0 support
Physical and Security BIOS Level Security Features	BIOS controlled electro-mechanical or equivalent internal chasis lock for the system. OR Software enabled /Chasis intrusion system/ TPM Lock or equivalent. BIOS based Ports enable/disable feature.
	BIOS Integrity checking – BIOS Protection to ensure that only trusted BIOS code is executed and not rootkits, viruses and malware.
	Verification done on boot up, shutdown and while the system is on.
	Automatic repair of BIOS if corrupted or compromised.
	Audit enabled - System Audit via Event Logs to capture data such as incident, repair date and time for troubleshooting and investigating
Ports	Minimum 6 X USB 3.0 or Higher, 1 X 1Gbps LAN Port", Preferably maximum USB ports on the front
Bays and Slots	Minimum 3 PCIe Gen 3 Slots, Minimum 1 M.2 Slots , Minimum 1 Internal/ External Bays
Operating System	Should have preloaded Genuine Win 10 Pro 64 WKST (or latest version of window os). All drivers required for proper integration of components should be supplied by the vendor. All latest drivers should be available to download from vendor's website.
	System should support for Red Hat® Enterprise Linux Desktop and Ubuntu
Form Factor	Convertible Mini Tower /Tower/SFF.
	System should feature Active Acoustic Reduction, with low noise level in accordance with ISO 9296 (tested in accordance with ISO 7779)
Remote Collaboration Capability	SI-H/OEM should provide the functionality/facility that the same document can be shared, accessed and updated simultaneously, by multiple users at multiple locations. Third party solution is also acceptable.
	Application should be stateless and should not transfer actual data over the network for security
	Should work on both Linux and Windows, and should be inter-operable.
Additional Software	1. The hardware vendor should supply an automatic system performance tuning and monitoring software on Windows.
	2. The tuning software should have modules for resource monitoring over a long period of time, and should be capable of showing GPU utilization (GPU, Graphics memory and Codec activity) for both Graphics and GPU Compute cards.

	3. A complete Offline Diagnostics and Asset Discovery software suite should be supplied along with the system.
Dust Filter	OEM should provide serviceable dust filter for avoid workstation failures due to dust and it should be connected into the workstation
Certifications	Window OS and Linux Certification, EPEAT India Registered
Display/ Monitor	23.8" FHD LED TFT or Better- Should be from same brand as the workstation

ORGI

Annexure – C7: Mono Laser Printer

Function	Print Only
Printing Technology	Laser A4 Mono
Print Speed – A4 (ppm)	55 ppm or Higher
Duplex Print Speed – A4 (ppm)	45 ppm or higher
Print Resolution	Up to 1200 x 1200 dpi
FPO from Ready - Black (Sec)	10 sec or less
Processor (MHz)	1.2 GHz or higher
Memory (standard)	512 MB or higher
Monthly Duty Cycle	Minimum 250,000 pages
Print Language	PCL 6, PCL 5, Postscript Level 3 emulation, native PDF printing
Input Capacity (sheets)	100-sheet multipurpose tray 1, 500-sheet input tray 2, 500-sheet input tray 3
Output Capacity (Sheets)	500-sheet output bin
Direct mobile printing	Embedded Wi-Fi Direct5/Bluetooth Low Energy8
Both side Printing	Automatic Duplex
Connectivity	1 Hi-Speed Device USB 2.0; 1 x 1GBaseT
Network protocols	TCP/IP, IPv4, IPv6; Print: TCP-IP port 9100 Direct Mode, LPD
Cartridge Technology	Composite

Note: Driver and Power Cables should be included in above specifications.

Annexure – C8(a): MFP – Multifunction Mono Printer

(B/W printing, faxing & Copying Color Scanning and digital sending (LaserJet Printer, Scanner, Fax, Copier & digital sending (All in one) A4 Size

Functions	Print, Copy, Scan
Print speed black (ISO, A4)	55 ppm or higher
First page out black (A4, ready)	As fast as 7 Sec
Duty cycle (monthly, A4)	250,000 pages or higher
Print technology	Laser
Print quality black (best)	1200 x 1200 dpi or higher
Processor speed	1.0 GHz or Higher
Display	Color Graphics Display (CGD) with touchscreen
Connectivity, standard	1 Hi-Speed Device USB 2.0,1 Gigabit Ethernet port
Memory	1.5 GB or higher
Input capacity	100-sheet multipurpose feeder, 500-sheet input feeder
Output capacity	500-sheet output feeder
Duplex printing	Yes
Duplex Scanning	Yes
Hard Disk	320 GB or higher
Scan resolution, optical	Optical: 600 dpi or higher
Automatic document feeder capacity	100-sheet or higher
Digital sending standard features	Scan to E-mail; Save-to-Network Folder; Save-to-USB drive; Send to SharePoint, Send to FTP, Send to Internet Fax; Local Address Book; SMTP over SSL; Blank Page Removal; Edge Erase; Auto Color Sense; Auto Crop to Content; Compact PDF
File Format Supported	PDF, Hi-Compression PDF, JPEG, TIFF, MTIFF, XPS, PDF/A
Scan speed (A4)	60 ppm/111 ipm or higher
Copy speed (black, A4)	55 cpm or higher
Cartridge technology	Composite

Annexure – C8(b): MFP – Multifunction Colour Printer

(Colour printing, Faxing & Copying Color Scanning and digital sending LaserJet Printer, Scanner, Fax, Copier & digital sending (All in one) A4 Size

Functions	Fax, Print, Copy, Scan
Print speed black and colour (ISO, A4)	45 ppm or higher
First page out black and colour (A4, ready)	As fast as 7 Sec
Duty cycle (monthly, A4)	100,000 pages or higher
Print technology	Laser
Print quality black and colour (best)	1200 x 1200 dpi or higher
Processor speed	1.0 GHz or Higher
Display	Color Graphics Display (CGD) with touchscreen
Connectivity, standard	1 x USB 2.0 and 1 x Gigabit Ethernet port
Memory	1.5 GB or higher
Input capacity	100-sheet multipurpose feeder, 500-sheet input feeder
Output capacity	500-sheet output feeder
Duplex printing	Yes
Duplex Scanning	Yes
Hard Disk	320 GB or higher
Scan resolution, optical	Optical: 600 dpi or higher
Automatic document feeder capacity	100-sheet or higher
Digital sending standard features	Scan to E-mail; Save-to-Network Folder; Save-to-USB drive; Send to SharePoint, Send to FTP, Send to Internet Fax; Local Address Book; SMTP over SSL; Blank Page Removal; Edge Erase; Auto Color Sense; Auto Crop to Content; Compact PDF
File Format Supported	PDF, Hi-Compression PDF, JPEG, TIFF, MTIFF, XPS, PDF/A
Scan speed (normal, A4)	75 ppm or higher
Copy speed (Black & Colour, A4)	45 cpm or higher
Cartridge Technology	Composite

Annexure – C9: SAN Switch for 3 Main Data Centres

Specifications for SAN Switch for 3 Nos. Main Data Centres at Delhi, Bengaluru & Lucknow

S. No	Minimum Specifications
1	PERFORMANCE : Auto- sensing 16 Gbps FC
2	PORTS : 48 Fiber port activated from day-1
3	SWITCH BANDWIDTH : Minimum 250Gbps (full duplex)
4	PROTOCOL SUPPORT : Fiber Channel
5	HIGH AVAILABILITY : Hot Plug, non-disruptive software upgrades, Redundant power supply
6	MANAGEMENT: Quick Configuration Wizard / CLI Management. Switch managed over 10/100
7	MEDIA TYPE : SFP, (Required FO patch cords to be supplied for complete connectivity as per solution architecture)
8	NETWORK SERVICE : Up to 16 Virtual SAN, Fiber Channel ping and port level statistics
9	FABRIC SERVICE : Name Service, Registered State Change Notification
10	Dual Port Power Supply

ORGI

Annexure – C10: Core Switch Type 1 for 3 Main Data Centres

Specifications for Core Switch for 3 Nos. Main Data Centres at Delhi, Bengaluru & Lucknow

Sr. No	Specifications
1	Layer-3 Rack mountable Chassis based LAN Switch
a	48 Port 10/100/1000 Base T Ethernet module – 1 unit
b	Fully populated 10GbE module with SR transceiver – 1 unit
c	Support for minimum 8 port 40GbE QSFP+ for future
d	Redundant Management/Processor Module
e	Hot swap-able Redundant Power Supply (Support for full system capacity)
2	Network OS Support should have inbuilt features as mentioned below static
a	**IPV4**: IP routing protocols like RIPv2, and OSPF, BGP v4, equal cost routing
b	**IPv6:** OSPFv3, and static routes. IPv6 Routing, management
c	**IEEE** 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad
d	IGMP snooping v1, v2 and v3
e	VLAN >1000
f	**Security :**802.1x with port security, mac filtering, DHCP snooping, Syslog, port security based on mac address, SSHv2, Per port broadcast, unicast and multicast storm control, VLAN ACLs, DHCP Interface Tracker (Option 82); Dhcp server to serve the Desktops
g	**Management** : SNMPv1, SNMPv2c, and SNMPv3 , traceroute, TFTP, Network Timing Protocol (NTP), RMON I and II , CLI support, Telnet
h	Support for External RADIUS /TACACS for console access restriction and authentication
i	**QoS** : 802.1p CoS and DSCP, Strict priority queuing, rate limiting, QoS for egress and ingress traffic
j	**Multicast :**Protocol Independent Multicast (PIM) for IP Multicast routing, including PIM sparse mode (PIM-SM) / PIM dense mode (PIM-DM) / PIM sparse-dense mode
k	Standard and Extended IP security access control list
l	Ingress and egress access-list
3	Non-blocking backpane
4	Core and access switch should be from same OEM.

Annexure – C11: Core Switch Type 2 for 18 Data Capture Centres

Specifications for Core Switch for 18 Nos. Data Capture Centres

Sr. No	Specifications
1	Layer-3 Rack mountable LAN Switch
a	24 Port 10/100/1000 Base T Ethernet
b	12 Port 10GbE (SR SFP+ module fully populated) scalable to 24
c	Hot swap-able Redundant Power Supply (Support for full system capacity)
2	Network OS Support should have inbuilt features as mentioned below static
a	**IPV4**: IP routing protocols like, RIPv1, and OSPF, BGP v4, equal cost routing
b	**IPv6:** OSPFv3, and static routes. IPv6 Routing, management and MLD Snooping
c	**IEEE** 802.1d, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.1ab, 802.3ad
d	IGMP snooping v1, v2 and v3
e	VLAN >1000
f	**Security :**802.1x with port security, mac filtering, DHCP snooping, Syslog, port security based on mac address,SSHv2,Per port broadcast, unicast and multicast storm control, VLAN ACLs, DHCP Interface Tracker (Option 82); Dhcp server to serve the Desktops,
g	**Management** : SNMPv1, SNMPv2c, and SNMPv3 , traceroute, TFTP, Network Timing Protocol (NTP), RMON I and II , CLI support, Telnet
h	Support for External RADIUS /TACACS for console access restriction and authentication
I	**QoS** : 802.1p CoS and DSCP, Strict priority queuing, rate limiting, QoS for egress and ingress traffic
j	**Multicast :**Protocol Independent Multicast (PIM) for IP Multicast routing, including PIM sparse mode (PIM-SM) / PIM dense mode (PIM-DM) / PIM sparse-dense mode
k	Standard and Extended IP security access control list
l	Ingress and egress access-list
3	Non-blocking backpane
4	Core and access switch should be from same OEM.

Annexure – C12: Access Switch

Sr. No.	Specifications
1	Access Switch should have 48 ports of 100/1000 RJ45 and min. 2 ports of 10G (2 SR SFP+ populated for uplink).
2	The Access switch should support VLANs.
3	The Access Switch should support minimum stacking/ MLAG of 4 units or higher. Cost of the stacking modules/Ports should be included.
4	The Access Switches should support link aggregation across the stack.
5	The connected servers or switches should be attached using standard LACP for automatic load balancing and high availability.
6	The Access Switch should support full Layer-2 features like STP, RSTP, MSTP, LAG, LACP, ACL, QoS, OSPF.
7	Shall be EAL / NDPP certified at the time of bidding.
8	The Access Switch should support IPv6 management features like IPv6 ping, IPv6 trace route, IPv6 Telnet, IPv6 TACACS, IPv6 DNS and IPv6 RADIUS.
9	Core and access switch should be from same OEM.

ORGI

Annexure – C13(a): Storage of 1PB for 3 Data Centres

Indicative specifications of Smart Rack are provided in Annexure-C28, however, Bidder & OEM of 1PB Storage should provide the Smart Rack (as Third Party) Solution in terms of power, cooling, firefighting, water leakage safeguards and rack space etc., in accordance to the equipment proposed at Data Centre Lucknow and Bengaluru, as 1PB Storage at these Data Centres are to be installed within the Smart Rack.

Sr. No.	Parameter	Functionality
1	Converge / Unified Storage	1. Offered array shall be an enterprise class high end storage, true converge / unified storage with File and block services respectively with active-active multi controller architecture. If any additional hardware required for file services, the same number of file controller shall be provided in High Availability.
		2. Offered Storage Array shall be supplied with minimum of Quad Crossbar Engines / Quad controller node / Quad controller engine or equivalent and shall be scalable to at-least 8 Crossbar engines/Controller nodes.
		3. Only Monolithic or Modular architecture shall be offered. In case of Modular architecture, only tightly coupled clustered storage implying integrated physical backplane or switching fabric or internal bus (into which different storage controllers are connected) would be considered. No loosely coupled clustered storage/ scale out storage architecture having external SAN or Ethernet switch for intra SAN connectivity is to be offered.
2	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms including: *Windows Server 2012 / 2016, VMware, Solaris, HPE-UX and IBM-AIX etc.*
3	Capacity & Scalability	1. The Storage Array shall be offered with 1000TB (1PB) of usable Capacity using 40% SSD / Flash drives RAID 6, 60% SAS 10K RPM or higher on RAID 6.
		2. Offered Array shall be scalable to at-least minimum of 1,900 numbers of Drives and shall be scalable to minimum 5 PB of raw capacity.
		3. Offered array shall support at-least 1PB usable capacity for file operations.
4	Cache	1. Offered Storage Array shall be given with at-least 1.2 TB DRAM Cache in a single array for both Data and control operations and shall be scalable to minimum 2TB DRAM Cache. DRAM cache should be protected. DRAM may be used for both read and write operations without de-gradation in the performance.
		2. Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache. In case offered storage use cache for OS, then additional cache should be provided. Self Certification/Undertaking by the OEM must be provided.
5	Processing Power	Offered Storage architecture shall such that there shall be no load on the storage CPU during Raid Parity calculations. In case, the controller CPU are used for RAID parity calculation, additional controllers shall be supplied on day1. Self Certification/ Undertaking by the OEM must be provided.
6	Architecture & Processing Power	The offered storage array shall be single array which is truly symmetric active-active with multi-controller architecture providing load balancing of IOPs and single LUN across all the controllers.

7	No Single point of Failure	Offered Storage Arrary shall be configurable in a No Single Point of Failfure (SPOF) configuration including Arrary Controller card, Cache memory, FAN, Power supply etc.
8	Disk Drive Support	1. Storage should support Flash Drives 1.92 TB to 15 TB atleast. Storage should support SAS Drives 1 TB to 1.8 TB atleast. All above drives should be hot-pluggable.
		2. Offered Storage array shall be truly optimized for flash operations and shall support minimum of 1000 Solid State disks / Flash disks.
9	Raid Support, Virtualization & No. of Volumes	1. Offered Storage Subsystem shall support Raid 1, 5 and Raid 6
		2. Offered storage array shall have virtual/thin pool support so that Raid 1, Raid 5, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application.
		3. Offered storage array shall support at-least 8000 Volumes per controller/32,000 volumes per array for host allocation, local replication and for remote replication.
10	Data Protection	In case of Power failure, Storage array shall have de-stage feature to avoid any data loss.
11	Centralized Monitoring	1. Offered storage shall have centralized monitoring engine for proactive Storage management.
		2. Centralized Monitoring engine shall have capability to provide following:
		a. Providing Firmware upgrade and patch upgrade recommendations proactively.
		b. Providing historical capacity and performance trend analysis.
		c. Shall be able to provide the executive Dashboard covering various critical and must aspects of Total Capacity, overall health / wellness score of array. De-duplication and compression ratio, over-all front-end performance etc.
12	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, SMB 3.0, NFS V4, FTP/FTPS etc.
13	Host Ports, Back-end Ports and Volumes	1. Offered Storage shall also natively support 32Gbps/16Gbps FC Ports, 10Gbps ISCSI and 10Gbps NAS (For File operations) ports.
		2. Offered Storage array shall be supplied with minimum of 16 x 16Gbps FC ports or 8 x 32Gbps FC ports for host connectivity, 4 x 10 Gb iSCSI ports and 8 x 10Gbps Ethernet ports for File operations. All type of Ports shall be 100% scalable.
		3. Offered Storage shall be supplied with at-least 576 Gbps aggregate throughput of backend connectivity using 6/12 Gbps ports and shall be at least 25% scalable.
		4. Offered storage shall be supplied with minimum four additional 10Gbps IP ports for storage based replication on Storage array and shall be scalable to at-least 8 x 10Gbps IP ports. " or Offered via FCIP rotuers in HA with min four additional 10Gbps IP ports for storage based replication on Storage array and shall be scalable to at-least 8 x 10Gbps IP ports.
14	Host Ports & Back-end Ports Cards	Offered storage shall have separate adapters for Host ports and back-end port cards for better ratio of high availability.

15	Global Hot Spare	1. Offered Storage Array shall support distributed Global hot Spare for offered Disk drives.
		2. Offered Storage Array shall support distributed Global hot Spare disk/capacity for each offered 24 Disk drives.
16	Performance and Quality of service	1. Storage shall be provided with Performance Management Software.
		2. 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.
17	Thin Provisioning and Space Reclaim	1. Offered storage array shall have support for Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time.
		2. 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.
18	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
19	Integration – Container	Offered Storage array shall be integrated with Docker, Red-hat OpenShift, Kubernetes and MESOS container technologies. Vendor shall support at-least following functionalities through their integration plugin. Third party solution is acceptable without degradation in performance.
		a. Multiple arrays support so that within a given cluster using a common configuration file on container platform. Third party solution is acceptable without degradation in performance
		b. Snap shot and clone
		c. Replication. Plugin shall allow to define the replication configuration on the container. Third party solution is acceptable without degradation in performance.
		d. Shall have flexibility to import the non-container volume into the container. Third party solution is acceptable without degradation in performance
		e. Container as a service from Storage array where vendor shall be able to define partition on the storage and shall be visible to container. Third party solution is acceptable without degradation in performance
		f. Support for both Fiber channel as well as ISCSI.
20	Snapshot / Point in time copy / Clone	1. Offered Storage shall have support to make the snapshot and full/thin copy (Clone) on the thin volumes if original volume is created on thick or vice-versa.
		2. The storage array should have support for both controller-based as well as file system based snapshots functionality (At-least 256 copies for a given volume or a file store).
21	Quota Management	For file services operations, offered storage shall support both user level as well as file level hard and soft quota.
22	Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software.
		2. Software shall be able to manage more than one array of same family.
23	Storage Tiering	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online.

		2. 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.
24	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family.
		2. The Storage array shall also support three ways (3 Data Centers) replication to ensure zero RPO natively without using any additional replication appliance.
		3. The storage array shall support incremental replication after resumption of Link Failure or failback situations.
25	File Level retention and immutability	For file services operation, offered storage shall support file protection against accidental, premature, malicious deletion and modification of data using file locking mechanism of WORM.
26	Licenses	Storage subsystem shall be supplied with Thin Provisioning, Snapshot, Clone, Performance Monitoring, Online Raid Migration, Online Volume conversion (thin to thin compressed, thin to thin de-dup etc.), Quality of services, Sub-Lun Tiering and File services on day 1 for the maximum supported capacity of array. Storage should support Encryption. Third party solution is acceptable without degradation in performance.

ORGI

Annexure – C13(c): Storage for 18 Data Capture Centres

Specifications of Storage of 50/75/100 TB for 18 Nos. Data Capture Centres

Bidders quoting external storage should also provision for SAN switch and FC cables, etc. (Applicable only in case bidder is quoting external storage):

Sr. No.	Parameter	Functionality
1	Converge/ Unified Storage	1. Offered array shall be a true converge / unified storage with File and block services respectively with active-active multi controller architechture. If any additional hardware required for file services, the same number of file controller shall be provided in High Availability.
		2. Offered Storage array shall be end-to end 12Gbps enabled which means that both Front-end Fiber channel ports and Back-end engines shall be operated at minimum 12Gbps speed.
		3. Proposed storage should support scalability to additional controller pair without using any kind of federation, with/without external virtualisation and not using loosely coupled clustered storage controllers/Scale out architecture having external SAN or ethernet switches for infrastructure SAN connectivity.
2	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms including: *Windows Server 2012, Windows 2016*, Vmware, Solaris, HPE-UX, IBM-AIX and Linux.
3	Capacity & Scalability	1. The Storage Array shall be offered with ----TB usable Capacity using 20% SSD drives RAID 6, 80% SAS 10K RPM or better on RAID 6. (Capacity may be referred from Annexure C-1 for respective location)
		2. Storage shall be scalable to at least 1PB usable capacity using 1.8/ 2.4TB or higher drives.
		3. Offered Storage array shall support at-least 240 SSD/Flash drives.
		4. Offered storage array shall support at-least 500 TB usable capacity for file operations.
4	Cache	1. Offered Storage Array shall be given with Minimum of 128 GB cache in a single unit and shall be scalable to 512 GB without any controller change.
		2. Cache shall be completely dynamic for read and write operations and vendor shall not offer any additional card / module for write cache operations.
		3. Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache. In case offered storage use cache for OS, then additional cache should be provided.
		4. Offered Storage array shall also have additional support for Flash Cache /Easy Tiering/Auto Tiering using SSD / Flash drives. Both File services as well as Block operations shall be able to utilize Flash Cache/Easy Tiering/Auto Tiering. Minimum 1TB Flash cache/Easy Tiering/Auto Tiering shall be supported.
5	Processing Power	Offered Storage architecture shall such that there shall be no performance degradation during Raid Parity calculations. In case of any performance degradation, additional source to be provided.

6	Architecture & Processing Power	Offered Storage array shall be true active-active so that a single logical unit can be shared across all offered controllers in symmetrical/asymmetrical fashion, while supporting all the major functionalities like Thin Provisioning, Data Tiering etc.
7	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
8	Disk Drive Support	Offered Storage Array shall support dual-ported 300 / 600 / 1200 /1800GB hot-pluggable Enterprise SAS hard drives, Minimum of 400GB SSD Drives along with nearline SAS 2TB / 4TB / 6TB / 8TB drives.
9	Raid Support, Virtualization & No. of Volumes	1. Offered Storage Subsystem shall support Raid 1/10, 5 and Raid 6.
		2. Offered storage array shall have virtual/thin pool support so that Raid 1, Raid 5, Raid 6 can be carved out from a logical space instead of dedicating separate physical disks for each application.
		3. Offered storage array shall support at-least 2000 Volumes per controller or 4000 volumes per Arrary.
10	Centralized Monitoring	1. Offered storage shall have centralized monitoring engine for proactive Storage management.
		2. Centralized Monitoring engine shall have capability to provide following:
		a. Providing Firmware upgrade and patch upgrade recommendations proactively.
		b. Providing historical capacity and performance trend analysis.
		c. Shall be able to provide the executive Dashboard covering various critical and must aspects of Total Capacity, overall health / wellness score of array. De-duplication and compression ratio, over-all front-end performance etc.
12	Data Protection	In case of Power failure, Storage array shall have de-stage feature to avoid any data loss.
13	Protocols	Offered Storage array shall support all well-known protocols like FC, ISCSI, SMB 3.0, NFS V4, FTP/FTPS etc.
14	Host Ports and Back-end Ports	1. Offered Storage shall have minimum of 4 x 16Gb, 4 x 10Gbps ISCSI and 4 x 10Gbps IP (Ports for file operations) host ports for connectivity to servers. All types of ports shall be 100% scalable.
		2. Offered storage shall have two additional IP ports for the the storage based replication.
		3. Offered storage shall support 32Gbps FC front-end ports also, if required in future.
		4. Offered storage shall have minimum of 16 SAS lanes running at 12Gbps speed and shall be scalable to 32 SAS lanes without any controller change.
16	Global Hot Spare	1. Offered Storage Array shall support distributed/dedicated Global hot Spare for offered Disk drives.
		2. Global hot spare shall be configure as per industry practice.
17	Performance and Quality of Service	1. Shall have capability to use more than 30 drives per array group or raid group for better performance.
		2. 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.

18	Thin Provisioning and Space optimization	1. Offered storage array shall support Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity.
		2. Offered Storage array shall support data reduction feature of De-duplication and Compression for thin volumes running on Solid state drives. Vendor shall support both de-duplication and compression on a given volume simultaneously.
		3. 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.
19	Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
21	Integration - Container	b. Snap shot and clone
		d. Shall have flexibility to import the non-container volume into the container.
		e. Container as a service from Storage array where vendor shall be able to define partition on the storage and shall be visible to container.
		f. Support for both Fiber channel as well as ISCSI.
20	Snapshot / Point in time copy / Clone	1. Offered Storage shall have support to make the snapshot and full/thin copy (Clone) on the thin volumes if original volume is created on thick or vice-versa.
		2. The storage array should have support for both controller-based as well as file system based snapshots functionality (At-least 256 copies for a given volume or a file store).
21	Quota Management	For file services operations, offered storage shall support both user level as well as file level hard and soft quota.
22	Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software.
		2. Software shall be able to manage more than one array of same family.
23	Storage Tiering	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online.
		2. 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.
24	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family.
		2. The storage array shall support incremental replication after resumption of Link Failure or failback situations.
25	File Level retention and immutability	For file services operation, offered storage shall support file protection against accidental, premature, malicious deletion and modification of data using file locking mechanism of WORM.
26	Licenses	Storage subsystem shall be supplied with Thin Provisioning, Snapshot, Clone, Performance Monitoring, Online Raid Migration, Online Volume conversion (thin to thin compressed, thin to thin de-dup etc.), Quality of services, Sub-Lun Tiering and File services on day 1 for the maximum supported capacity of array.

Annexure – C14: Backup Software

Sr.No	Specifications
1	The proposed backup solution should be available on various OS platforms such as Windows, Linux and UNIX platforms.
2	The proposed backup solution should be for 40% of Total backup appliance capacity.
3	The proposed backup software should support both backups using snapshot/hardware based and software based as well as backup to tapes for long term and offline data retention.
4	The backup software should be capable to supporting 99,999 backup sessions in day.
5	The proposed backup software should automatically secure the communication between the server and the client using Encrypted Control Communication
6	The backup software should be capable of supporting 1000 concurrent sessions.
7	The backup software should be able to support maximum of 40 Million files per directory.
8	The proposed backup software should support single management window for all the different data protection locations.
9	The proposed backup solution shall have same web based GUI across heterogeneous platform to ensure easy administration.
10	The proposed backup solution should support tape mirroring of the same job running concurrently with primary backup.
11	The proposed backup software should use web-based scheduler for the backup jobs.
12	The proposed backup software should support the use REST API for browse and restore operations.
13	The proposed backup solution should allow creating tape clone facility after the backup process.
14	The proposed backup solution shall be configured in such a fashion that no extra license for customer and media servers is required while moving from LAN to SAN based backup and adopting new Data Bases and OS in future.
15	The proposed backup solution shall be configured with unlimited customer and media licenses for both SAN based backup and LAN based backup and adopting new Data Bases and OS in future.
16	The backup software should support the Capacity based model or Application based model of licensing.
17	The proposed backup solution supports the capability to write minimum 30 data streams.
18	The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to customer/servers.
19	The proposed backup solution has in-built media management and supports cross platform device and media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
20	The proposed backup solution has certified “hot-online” backup solution for different type of Enterprise databases and applications.

21	The proposed backup solution shall also support granular recovery for VMware, Exchange server, Share point Portal.
22	The backup software should support Non Staged Granular recovery in VMWare.
23	The proposed backup software should use the same API for software and hardware deduplication.
24	The backup software should support backup to disk /VTL / Deduplication Device via fibre channel, IP (NFS & CIFS etc.).
25	The proposed backup software should support both on premise and secure hosted backup solution.
26	The proposed backup solution shall support automatic skipping of backup during holidays.
27	The backup software should support the option of prioritizing backups.
28	The backup software should support missed job execution.
29	The Backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions.
30	The Backup software should support object copy of File system data to Microsoft Azure.
31	The backup software should support Automated Replication Synchronization of meta data between different site and across devices like HPE/EMC via Catalyst or Boost.

Annexure – C15(a): 200TB Backup Appliance for Data Centre, NDC, ORGI

Sr.No	Specifications
1	Offered Disk to disk backup device shall be Modular design to allow configuration, add capacity increase performance.
2	Offered appliance shall be certified to work with offered Backup software application vendor.
3	Offered device shall be offered with Minimum of 200TB of Usable space scalable to at-least 800TB Usable.
4	Offered device shall be offered with Minimum of 200TB of Usable space scalable to at-least 800TB Usable without degradation in performance
5	Offered device shall have separate dedicated drives for Operating System of appliance and shall not participate in data backup.
6	Offered device shall be protected with hardware raid 6 from the factory so that no raid configuration is required in field for data drives. Min. one Hot spare drive shall be offered.
7	Offered device shall be offered with dual Hardware Raid Controller card. Each card shall have dual 12Gbps SAS ports or equivalent backend bandwidth using 6/12Gbps SAS interface.
8	Offered device shall support emulation of both VTL and NAS target like NFS & CIFS etc.
9	Offered device shall have the ability to configure at-least combination of 30 tape Libraries & NAS targets along with 30,000 or more Cartridge slots in the single appliance.
10	Offered device shall have capability to deliver selective restore from disk Library itself.
11	Offered device shall have integrated de-duplication license, low bandwidth replication license so that only unique non duplicated block transfers to remote / DR location.
12	Offered device shall have intelligence to understand both source based and target based de-duplication and shall be integrated with all well-known backup ISVs like Veritas, Commvault and Veeam etc. At-least 3 ISVs shall be supported.
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.
14	Ability to flexibly emulate tape drive/ tape formats LTO-Gen5/LTO-Gen6/ LTO-Gen7 etc.
15	Offered device shall have Minimum of 4 x 25/10Gbps & 4 x16/ 32Gbps FC and minimum of 2 x 1Gbps IP connection. License and SFP for all ports shall be offered and configured.
16	Offered Appliance Fiber channel ports shall support connectivity of servers either directly or via SAN switches while supporting the both source and Target based de-duplication.
17	Offered disk based backup device shall also support encryption functionality.
18	Offered disk based backup appliance shall support VLAN tagging. Offered IP ports of same type shall also support Port bonding in Adaptive Load balancing as well as in Active-backup

	mode.
19	When fully populated, offered device shall support rated write performance of more than 20TB per hour in native mode.
20	When fully populated, offered device shall support rated write performance of more than 32TB per hour in native mode.

ORGI

Annexure – C16: On-line Modular UPS Type 1

Specifications for Online Modular UPS with Capacity 60 KVA with N+1 Module Level Redundancy

General Specifications	
Rating	60KVA Modular UPS with N+1 module level redundancy
UPS Topology	On line double conversion VFI SS 111
Architecture of the UPS	Modular, scalable, redundant based minimum rating of Power Modules 20KVA. Each rated module should be further splited into three granular modules of equal capacity
Technology	Multi Controller design, Hot/Safe swappable modules, Unity power factor IGBT based Rectifier & Inverter
Neutral	Neutral Passing through
Output wave form on mains run	Sinusoidal
Output wave form on battery run	Sinusoidal
Bypass type	Static and electro-mechanic
Transfer time	Zero
Input	
Nominal Voltage	400 V three phase + N
Voltage range	- 20% +15%
Frequency	50 Hz o 60Hz
	(autosensing)
$THDI_{in}$	< 3%
Power Factor	> 0.99
Output	
Nominal voltage	400 V three phase + N
Nominal power	60 KVA
Active power	60 KW
Output PF	Unity
AC-AC Efficiency (On Line)	up to 96%
Voltage variation (static)	± 1%
Voltage variation	± 1%
THDv on nominal power (linear load)	<1%
THDv on nominal power (not linear load P.F.=0,7)	< 1 %
Frequency	50 Hz o 60 Hz (autosensing or selectable)
Frequency tolerance	Synchronized with input frequency or
	± 1% free run
Current Crest Factor	3:1 accordingly with IEC EN62040-3
Overload capability: @ Unity PF	
· 10 min	115% load rate with no bypass intervention
· 1 min	135% load rate with no bypass intervention
Battery	
Type	Lead Acid, sealed, free maintenance VRLA
Backup	30 min
Min VAH	72000VAH
	Minimum 2 strings of batteries to avoid single bank failure,

Environmental specs	
Noise level @ 1m	<65 dBA
Working temperature range	from 0°C to +40°C
Stock temperature range	from -20°C to +50°C (excluded batteries)
Humidity range	20-95% not condensing
Protection degree	IP21
Input/Output connections	3P + N + PE Connectors on omega bar
Standards	EN 62040-1, EN 62040-2, EN 62040-3 , UE

ORGI

Annexure – C17: Online Modular UPS Type 2

Specifications for Online Modular UPS with Capacity 80 KVA with N+1 Module Level Redundancy

General Specifications	
Rating	80KVA Modular UPS with N+1 module level redundancy
UPS Topology	On line double conversion VFI SS 111
Architecture of the UPS	Modular, scalable, redundant based minimum rating of Power Modules 20KVA. Each rated module should be further splited into three granular modules of equal capacity
Technology	Multi Controller design, Hot/Safe swappable modules, Unity power factor IGBT based Rectifier & Inverter
Neutral	Neutral Passing through
Output wave form on mains run	Sinusoidal
Output wave form on battery run	Sinusoidal
Bypass type	Static and electro-mechanic
Transfer time	Zero
Input	
Nominal Voltage	400 V three phase + N
Voltage range	- 20% +15%
Frequency	50 Hz o 60Hz (autosensing)
$THDI_{in}$	< 3%
Power Factor	> 0.99
Output	
Nominal voltage	400 V three phase + N
Nominal power	80 KVA
Active power	80 KW
Output PF	Unity
AC-AC Efficiency (On Line)	up to 96%
Voltage variation (static)	± 1%
Voltage variation	± 1%
THDv on nominal power (linear load)	<1%
THDv on nominal power (not linear load P.F.=0,7)	< 1 %
Frequency	50 Hz o 60 Hz (autosensing or selectable)
Frequency tolerance	Synchronized with input frequency or ± 1% free run
Current Crest Factor	3:1 accordingly with IEC EN62040-3
Overload capability: @ Unity PF	
· 10 min	115% load rate with no bypass intervention
· 1 min	135% load rate with no bypass intervention
Battery	
Type	Lead Acid, sealed, free maintenance VRLA
Backup	30 min
Min VAH	100800VAH
	Minimum 2 strings of batteries to avoid single bank failure,

Environmental specs	
Noise level @ 1m	<65 dBA
Working temperature range	from 0°C to +40°C
Stock temperature range	from -20°C to +50°C (excluded batteries)
Humidity range	20-95% not condensing
Protection degree	IP21
Input/Output connections	3P + N + PE Connectors on omega bar
Standards	EN 62040-1, EN 62040-2, EN 62040-3 , UE

ORGI

Annexure – C20: Online Modular UPS Type 5

Specifications for Online Modular UPS with Capacity 40 KVA with N+1 Module Level Redundancy

General Specifications	
Rating	40KVA Modular UPS with N+1 module level redundancy
UPS Topology	On line double conversion VFI SS 111
Architecture of the UPS	Modular, scalable, redundant based minimum rating of Power Modules 10KVA. Each rated module should be further splited into three granular modules of equal capacity
Technology	Multi Controller design, Hot/Safe swappable modules, Unity power factor IGBT based Rectifier & Inverter
Neutral	Neutral Passing through
Output wave form on mains run	Sinusoidal
Output wave form on battery run	Sinusoidal
Bypass type	Static and electro-mechanic
Transfer time	Zero
Input	
Nominal Voltage	400 V three phase + N
Voltage range	- 20% +15%
Frequency	50 Hz o 60Hz
	(autosensing)
$THDI_{in}$	< 3%
Power Factor	> 0.99
Output	
Nominal voltage	400 V three phase + N
Nominal power	40 KVA
Active power	40 KW
Output PF	Unity
AC-AC Efficiency (On Line)	up to 96%
Voltage variation (static)	± 1%
Voltage variation	± 1%
THDv on nominal power (linear load)	< 1%
THDv on nominal power (not linear load P.F.=0,7)	< 1 %
Frequency	50 Hz o 60 Hz (autosensing or selectable)
Frequency tolerance	Synchronized with input frequency or
	± 1% free run
Current Crest Factor	3:1 accordingly with IEC EN62040-3
Overload capability: @ Unity PF	
· 10 min	115% load rate with no bypass intervention
· 1 min	135% load rate with no bypass intervention
Battery	
Type	Lead Acid, sealed, free maintenance VRLA
Backup	30 min
Min VAH	45000VAH
	Minimum 2 strings of batteries to avoid single bank failure,

Environmental specs	
Noise level @ 1m	<65 dBA
Working temperature range	from 0°C to +40°C
Stock temperature range	from -20°C to +50°C (excluded batteries)
Humidity range	20-95% not condensing
Protection degree	IP21
Input/Output connections	3P + N + PE Connectors on omega bar
Standards	EN 62040-1, EN 62040-2, EN 62040-3 , UE

ORGI

Annexure – C21: Web Application Firewall

Sr No	Specifications
	Architecture
1	The proposed WAF should be a dedicated appliance
2	WAF should support below Performance parameters:
	a. 12M HTTP concurrent Request Per Second
	b. 30K SSL TPS or more with RSA2K Key and 20K or more with ECC
	c. 20Gbps of SSL Throughput and Compression Throughput
	d. Minimum 5Gbps of WAF throughput i.e. WAF throughput after applying WAF features asked in RFP
3	The proposed device should support up-to 5 Virtual Instances.
4	16 x 10 GbE SFP+ SR and support for 2x40G QSFP+ for future
	WAF should have the flexibility to be deployed in the following modes:
1	Reverse proxy and forward proxy
2	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode,
3	The solution must be able to handle OWASP Top 10 attacks, Anti-Bot Mobile DDoS protection and application layer encryption
	Hiding Sensitive Content Parameters:
1	It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)
2	WAF should support for IPv4 and IPv6 traffic
	Auto Policy Optimization
1	Policies must be automatically generated from auto learn results
2	Auto-learn options should be available to tweak and fine tune rules. The auto learn policy should have provision to put into staging mode for specific time period to avoid the false positive.
	Following Threats should be protected by the proposed WAF solution:
1	Parameters Tampering
2	Cookie Poisoning
3	SQL Injection
4	Should be able to protect Cookie Poisoning and Cookie Tampering.
5	Should protect certain hidden form fields.
6	Application Layer Encryption or any other mechanism/function to protect against Browser based Malware
7	API authentication and API Gateway protection
8	Protection against SYN-flood type of attacks
9	Buffer Overflow Attacks
10	Should have controls against Brute force attacks
12	Cross-Site Scripting (XSS)
13	Brute Force Attacks
14	Custom brute force attack detection for applications that do not return 401.
15	Antibot Mobile SDK to protect against Mobile app based bot

16	Cross Site Request Forgery (CSRF)
17	Must provide ability to allow or deny a specific URL access.
18	Ability to define different policies for different applications
19	Ability to create custom attack signatures or events
20	FTP and SMTP protocol protection. Third party solution is accepted
21	The proposed WAF should support the following Security Features/Functionalities:
22	Must support multiple HTTP versions such as HTTP/0.9, HTTP/1.0, HTTP1.1, HTTP 2.0 client side and server side both.
23	Should validate header length, content length, Body length, Parameter length, body line length etc.
24	The proposed solution should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioural analysis, server performance monitoring, and escalating JavaScript and CAPTCHA challenges/Device Finger Printing
25	WAF should support inbuilt capability or via integration with 3rd party solution to protect against the mobile/tablet application-based attacks through Anti-Bot Mobile SDK which whitelist establish trust based on an embedded software package within the application code and corresponding cookie verification to protect application against attacks generated from mobile
26	Client certificates should be supported in passive mode and active mode.
27	In termination mode, the backend traffic (i.e. the traffic from the WAF to the web server) can be encrypted via SSL
28	XML Security Protection and XML encryption feature
29	The WAF should have inbuild credential stuffing database to protect against compromised credentials
30	The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support proposed web application vulnerability assessment tolls to virtually patch web application vulnerabilities.
31	WAF should support inbuilt PCI DSS compliance
	WAF should provide the application visibility and reporting with below metrics and entity for each application:
1	Client IP addresses / subnets as well as geographical regions
2	Total Transactions as well as Average and Max Transactions/sec
3	Most commonly requested URLs
4	Server Latency and Page Load times
5	Virtual Server and Pool server performance
6	Page Load Time
7	Response code
8	OS and Browser
9	URL details
	OEM ELIGIBILITY CRITERIA
1	"Offered solution should be EAL or NDPP (Network Device Protection Profile) certified under Common Criteria Program for security related functions or ICSA Lab certified.

Annexure – C22: Database Activity Monitoring (DAM)

S.No	Requirement
1	The solution should be Database agnostic and should support at least the following databases: Oracle, SQL Server, Sybase, MySQL, IBM DB2
2	The solution should support on the following OS platforms at least: Microsoft Windows, Red Hat Enterprise Linux / Oracle Linux, HPUX, ORACLE SOLARIS
3	Solution does not require changes in the database application (e.g. truning audit or trace on)
4	Solution should be a non-intrusive agent installed on the server. The agent should read the data from shared memory
5	Solution should protect it-self from tampering and attacks
6	Solution allows easy translation of actual database activity into monitoring / audit policy direct from alerts
6.1	Solution should be capable of capturing the alerts which will include the following metadata:
6.2	Originating IP Address
6.3	DB User
6.4	OS User
6.5	Full SQL Statement
6.6	Accessed tables
6.7	Application Name
6.8	Module Name
6.9	Host Name/Terminal name
7	Solution should easily integrate with SIEM and other management products
8	Solution should be capable of monitoring of all database activities and protect against insiders with privileged access
9	Solution should offer granular monitoring of queries, objects and stored procedures with realtime alerts and prevention of breaches
10	Solution should provide protection against newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime and without having to update the patch itself.
11	Solution should offer flexible audit and reporting capabilities suitable for PCI DSS, SOX and HIPAA
12	Solution should provide multiple user roles that facilitate separation of duties
13	Solution should capable of monitoring and alerting unauthorized access to sensitive data on the Database, like credit card tables etc.
14	Solution should record all SQL transactions : DML, DDL , DCL and Selects and The ability to store this activity securely outside the database
15	Solution should have the ability to generate alert on policy violations and provide real time monitoring and rule based alerting.
16	Solution Should report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.

17	Solution Should report on database access including logins, client IP, server IP and source program information.
18	Solution Should track and report all failed logins.
19	The agent should not demand for restart of the database while installing or while upgrading or while uninstalling the solution
20	Solution should be able to monitor inter and intra DB activities and attacks
21	The solution should have a single console to manage and monitor database activity monitoring and the vulnerabilities inside the database
22	Solution should be capable of detecting weak passwords
23	Solution Application comes with predefined reports, allows for customizing and Ad-hoc reports
24	End user should be able to contact the OEM support directly via web and phone. The support should be based out of India.
25	The solution should be proposed with Premium Support with single point of contact directly from OEM for all post-sales issues. The same should be certified by OEM with relevant documents. OEM should provide quarterly health review of the solution.

ORGI

Annexure – C23: Patch Management Solution

Sr No	**Specifications**
1	Able to identify systems with other non-patch vulnerability conditions and identify these conditions without performing a network scan.
2	Product must provide pre-defined, out-of-box OVAL based policy definitions. (OVAL Definitions are standardized, machine-readable tests written in the Open Vulnerability and Assessment Language (OVAL) that check computer systems for the presence of software vulnerabilities, configuration issues, programs, and patches)
3	Allow the console user to deploy actions to remediate against the vulnerabilities identified.
4	Must be able to identify and fix the SANS Top 50 Vulnerabilities and also Windows registry Vulnerabilities.
5	The product must map all vulnerabilities to industry standards to provide CVE, CVSS references and link to National Vulnerability Database.
6	Able to target the Vulnerabilities based on any particular property retrieved.
7	**Security Policy Management (Windows)**
8	Able to identify agents that have various instant messengers and be able to uninstall them.
9	Able to remove and create network shares at any time.
10	Able to start and stop services on remote machine without user's knowledge.
11	Able to shut down or restart any machine targeted based on any system properties (e.g. user name, system location, by version of software installed, etc.)
12	Allow console user to customize the level of control using granular details like make of device or serial no. of device.
13	Should be able to support Windows and major applications
14	Ability to track installed applications on each agent, i.e. Applications that will run only if "Installed" on the computer
15	Ability to track standalone executable applications on each agent, i.e. Applications that do not need to be installed
16	The Analysis should include the following information (but not limited to) with the ability to drill down for more detailed views: a. Publisher name b. Software title name c. Software title version d. Total computers Count e. Total runs Count f. Total time g. Average runs h. Last used Time
17	Web UI should allow Role Based access to allow or restrict user's privileges by their role.
18	Web UI should have ability to view, filter, sort upon user input to create custom reports.
19	Ability to view all properties & raw data gathered from the agent during the inventory process.
20	Product must include a "Software ID Catalog" that identifies thousands of Standard publishers/ software vendors & their products.
21	Product must include a "Software ID Catalog" that allows for the entry of custom developed software titles.
22	Product must include a "Software ID Catalog" that allows for the custom classification of standard applications based on customer's preferences.

23	Ability to create groups based on inventory properties like (but not limited to): a. Active Directory path b. Subnet Address c. Operating System d. Inventory group membership e. Nested grouping must be supported
24	Ability to create License contracts based upon Software Titles
25	Custom fields must be able to be created for contracts to allow for the entry of unique data in the contract such as PO Number, Vendor Name, Asset Number etc.
26	Custom fields must be able to be created within License Contracts with the options to choose field attributes like: a. Selection list b. Checkboxes c. Radio Buttons d. Text Fields etc.
27	Ability to create License Compliance reports based on the details specified in License Contracts that were created.
28	The product must support the ability to export reports.
29	The product must be capable of generating license compliance reports for Windows and Non Windows OS platforms.
30	The product must be capable of generating software usage metering reports for Windows and Non Windows OS platforms.

ORGI

Annexure – C24: Host-based Intrusion Prevention System (for Servers)

HIPS is required on each Server/VM to protect at server level file system.

Sr. No.	Specifications
1	Host based Detection and Prevention System (HIPS) shall provide protection at the server level file systems.
2	It shall be deployed on all Server VM's.
3	It shall not impact the performance of the OS. Solution should support Linux & Windows for management server.
4	HIPS shall monitor systems in real time to detect and respond to security breaches and other unauthorized activities. It shall monitor transactions between the OS and other resources including the file system, network, memory and library modules.
5	It shall maintain the integrity of the OS by preventing unauthorized changes to executable files, command shell and registry.
6	HIPS shall provide centralized management tools for monitoring and enforcement of host - wide intrusion detection security policies.
7	HIPS shall protect the host against the following attacks - buffer overflows, trojan horses, irregular packets, malicious HTML requests, and worms etc.
8	Communication between the HIPS and management system shall be through a secure channel using SSL.
9	HIPS shall log all events for audit and analysis. It shall be able to send alerts to operators through the following mechanisms - GUI web screen, email message and through SNMP traps.
10	It shall be able to manage at least 500 host system sensors from a single manager.
11	It shall allow for the separation and delegation of security administrative tasks to different, specified individuals through role - based administrations.
12	It shall be able to scan Operating System and application log files, for footprints of malicious behaviour.
13	It shall have provision for addition and automatic / manual updation of existing signatures.
14	HIPS shall monitor the system level changes (Windows Registry in Windows Operating System) for any attempts to alter or delete it in any form.
15	It shall be able to protect servers, applications, file permissions and contents, file size etc. Multiple policy creation shall be supported. It shall be possible to activate / de activate certain policies. Deployment of the policies shall be dynamically possible.
16	The system shall be able to record all events especially intrusion events. Normal and abnormal events shall be recorded under separate heads.
17	It shall be possible to generate reports based on built in formats or new formats as defined by the administrator / user. Ad-hoc querying shall be supported.

Annexure – C25: SIEM (Security Incident & Event Management)

Sr No	Specifications
1	The Proposed solution can be in either appliance or software (alongwith hardware) platforms. In case of Software platform, bidder should factor hardware, OS, Database and storage any other license to support the SIEM solution including scalability with no additional cost to be borne by the customer.
2	The SIEM platform should be a Hardened Operating System Based solution with a clear physical separation of the collection engine, the logging engine and the co-relation engine. The solution should have a scalable architecture, catering multi-tier support and distributed deployments.
3	The solution should support both agent based and agent less architecture to collect the security logs across various resources and assets
4	The SIEM Correlation solution should be able to handle a minimum of 20,000 Sustained EPS and scalable to 30,000 without replacing existing hardware. 6 months of normalized log storage and 1 year of raw log storage.
5	For assets not natively supported, the SIEM solution should provide the collection of events through customization of connectors or similar integration; Must support event collection using at least the following industry standards: syslog, OPSEC, WMI, ODBC, FTP, SCP, HTTP, text file, CSV and XML file.
6	The SIEM receiver appliance or log collection appliance must store the data locally if communication with centralized correlators is unavailable.
7	The SIEM Solution should provide the capacity to maintain the Normalized logs online for six months.
8	Solution should be capable of retrieving the archived logs for analysis, correlation and reporting and for forensic purposes.
9	Receiver appliance should have the capability to collect flows.
10	Receiver appliances / Log collector should be able to work in high availability without the need for any third party solution for High Availability.
11	The proposed SIEM solution should integrate bi-directionally with the Servers such that the proposed SIEM solution should be able to change policies through integration on the proposed servers such as in case there is a virus outbreak, SIEM solution should be able to take down the malformed services or protocols in all or a segment of or individual server centrally.
12	Solution should have capability to audit any tampering of log collection in the SIEM solution.
13	The proposed solution should provide a minimum log compression of 75% for ensuring log compression to reduce overall log storage space for the raw log format
14	The SIEM solution should provide Native support for Incident Management Work Flow.
15	The solution should provide pre-defined report templates. The reports should also provide at least the following reports out of the box or customized for: ISO 27001-2, Basel II. Etc.
16	The solution should have inbuilt report for the NIPS, HIPS, End Point Security solution, etc including Attack Summary, Attacks over Time, Normalized Dashboard etc.
17	The solution should have inbuilt report for the Database security solution including DAM Privileged User Summary, DAM Event Details, DAM Failed Login Details, DAM User Account Change Summary
18	The SIEM solution should provide content aware correlation both rule based and rule less correlation against data collected from multiple devices across the network.
19	The SIEM Solution should provide real time threat intelligence from Own or other third party trusted feed vendors.
20	The solution should have pre-defined correlation rules out of the box, so as to provide correlation on the fly.
21	The solution should have pre-defined content packs which contain use-case driven correlation rules, alarms, views, reports, variables, and watchlists to address specific threat activity.
22	The filtering options should support Boolean operations including “OR, “NOT” and “AND” logic operations.

23	The SIEM solution must support the ability of integrating with at least one intelligence system with information from global risks and use the information collected in this system in the correlation of events.
24	The SIEM solution should provide a formula of threat which should be customized to allow increasing or decreasing the level of risk with at least the following types of correlation:
	A. Geo Location Based correlation
	B. Historical Based Correlation
	C. Vulnerability Based Correlation
25	The activities should be separated by levels of risk for the company. For example, Risk very high, high, medium, low and very low.
26	End user should be able to contact the OEM support directly via web and phone. The support should be based out of India.
27	The solution should be proposed with Premium Support with single point of contact directly from OEM for all post-sales issues. The same should be certified by OEM with relevant documents. OEM should provide quarterly health review of the solution.

ORG

Annexure – C26: End Point Protection and Remediation

Sr.No.	Specifications
1	Solution must scan, detect, clean, delete and quarantine the infected files.
2	The antivirus solution should provide scanning capabilities such as:
A	On access scanning
B	Real time scanning
C	On-demand scanning
D	Scheduled scanning
E	Compressed file scanning
F	Firewall
3	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:
A	Terminating all known virus processes and threads in memory
B	Removing any Microsoft Windows services created by viruses
C	Includes Cleanup for Spyware, Adware etc
4	The solution should be capable of doing client deployment via remote, Web UI, Login Script and Client Installer.
5	The solution should provide Role based administration.
6	The solution should provide quarantine management in order to prevent spreading. A management interface must be provided to allow the administrator to review, sort and analyze quarantined items.
7	Solution must provide to scan single file/directory/entire system and detect, clean, delete or quarantine the infected file.
8	Solution must provide scheduled scan configuration for full-disks scan at designated time from central manager for clean, delete or quarantine infected file.
9	Solution must provide to prevent endpoint users from uninstalling or disabling the managed antivirus services.
10	Solution must provide a utility program for clean uninstallation process of the corrupted antivirus.
11	Solution must provide virtualized environment
12	Solution must provide Endpoint based Intrusion Prevention System to proactively block and safely eliminate malwares and potentially unwanted program from endpoints.
13	Solution must allow for creating whitelisting of application programs, DLLs and executable files and block all remaining programs, DLLs. executable files for execution.
14	Solution must provide self-learning Whitelisting, and block applications attempting to execute on any endpoint, unless explicitly allowed by administrator.
15	Solution must provide prevention of tampering and hijacking of applications
16	Solution must provide to create classify applications which are attempting network access, and block unauthorized connections and data transfers by malicious programs.
17	Solution must provide to protect against zero-day attacks
18	Solution must provide to accept automatically new software added through authorized processes.

19	Solution must provide all the supported versions/latest versions of Microsoft Windows Operating Systems.
20	Solution must provide to generate user defined reports from database. In case reports are provided in raw logs, vendor must be able to generate meaningful reports by exporting into a database.
21	Graphical Charts for malwares, infected endpoints etc. for managed clients.
22	Solution must provide to integrate with 3rd Party Log Analyzer Application Software like SIEM.
23	Solution must provide a Utility program for all supported Windows, Linux and MAC operating systems for collecting logs of infected endpoints for analyzing and developing signatures.
24	Vendor must provide log analysis of infected systems and submit required suspected files to OEM lab for new signature
25	The Solution should check for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system.
26	Solution must provide Single agent for endpoint protection and EDR(endpoint detection & response) .
27	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.
28	Solution should perform analysis on “known" & "unknown" content. Scanning files using whitelisting, file hash reputation looking for known good & known bad content and send unknown files & URLs to sandbox for determination in a customized sandbox environment
29	The solution should have a centralized repository of all the portable-executable files in the organization. It should also provide the reputation information of the files.
30	OEM Must have Technical support team in India.
31	Vendor must provide software upgrades, new malware antivirus signatures, and technical know-how transfer training.

Annexure – C27: Data Leak Prevention System

Sr No	**Specifications**
1	The Solution should actively monitor the ways confidential/ sensitive data can be used on the endpoint and flags any activity not in accordance with policy defined from the centralized console also discovers that and move/copy to the central location.
2	The Solution should provide choices to address and remediate incidents and to operate in unobtrusive manner possible.
4	The Solution should scan laptop and desktop hard drives for confidential/ Sensitive data in order to inventory, secure or relocate it and provide templates or equivalent to enable out-of-the-box discovery of sensitive data mapped to different industry and regulatory directives.
5	The Solution should scan for confidential/sensitive data when endpoint is idle and subsequent scans must run on only those things that have changed since the previous scan.
6	The Solution should provide following detection technologies to address different types of data:
7	Content which looks for data matching keywords, expressions or patterns, file type and image text recognition, and other signature-based detection technologies.
8	Fingerprinting which looks for exact matches of whole or partial files, coming from structured sources (e.g. databases) and unstructured sources (e.g. design documents) that are fingerprinted with a hashing algorithm.
9	The Solution should monitor data being copied and pasted from the clipboard to prevent confidential/sensitive data from being pasted to specific application.
10	The Solution should provide trusted device support enables organizations to define specific removable media devices that can be used with confidential data, providing a more granular level of protection while still enabling required business functions.
11	The solution should provide broad remediation capabilities: onscreen pop-up notification; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the flexible response feature, such as applying encryption to a file.
12	The Solution should automatically notify data owners of the policy violation.
13	The Solution should have a web base management for defining, deploying, and enforcing data loss policies, responding to incidents, analyzing and reporting policy violations, and performing system administration.
14	The solution should detect whether data has been entered in forms such as tax, medical, or financial forms in various image formats, including PDF, JEPG, BMP, PNG and TIFF.
15	The solution should be able to restrict the number of files and/or total size of files attached to email.
16	The solution should enable to set limits on the size of indexes and to choose partial matching on specific profiles.
17	The solution should be able choose to scan all Box user accounts, or select the accounts including administrative and co-administrative accounts

18	The solution should be able to exclude specific printers from being monitored, including local, network, and PDF printers.
19	The solution should monitor mail communications and detects confidential/sensitive data that is being sent in violation of security policy. If a security policy is violated, it should route messages to an encryption gateway (optional), quarantines messages to a secure server, or blocks email communications.
20	The solution must redirect, quarantines, or blocks outbound messages containing confidential/ sensitive data. It must be deployed at egress points in the network DMZ and should integrate with your existing on premise, public or private cloud messaging infrastructure.
21	The solution must block or remove sensitive data from outbound web communications if they violate security policy.
22	The solution should integrate with HTTP/HTTPS, or FTP proxy servers using ICAP to detect and prevent confidential data in outbound web communications.
23	The solution should provide comprehensive protection for managed and unmanaged endpoints, including mobile devices that access the Web through your corporate network.
24	The solution must discover stored confidential data throughout the enterprise; monitor the ownership and use of stored data; and protect sensitive data according to centrally administered policies.
25	The solution should be used individually or together as a complete solution to reduce the risk of data loss.
26	The solution should discover and protect confidential data stored on file shares, databases, and repositories in data centers.
27	The solution should have encryption to encrypt entire disk and any sensitive data copied on the USB data should be encrypted.
28	The solution should have a technology that analyzes file access on network-attached storage (NAS) filers, Windows servers. It should identify and protect sensititive files and data.
29	The solution should recognize true file types. It should be able to recognize even of the extension was changed.
30	The solution should provide broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the flexible response feature, such as applying encryption to a file using the endpoint encryption flex response.
31	The solution should encrypt different types of removable media, including USB drives, external hard drives, and CD/DVD/Blu-ray media.
32	The solution encrypt all the drives and once encrypted, a user should only enter their passphrase once and single –sign-on technology should passes them through to their main screen, eliminating the need to re-input multiple passwords.

Annexure – C28: Smart Rack for DR at Lucknow & Bengaluru Data Centres

Indicative specifications of Smart Rack are provided below, however, Bidder & OEM of 1PB Storage should provide the Smart Rack (as Third Party) Solution in terms of power, cooling, firefighting, water leakage safeguards and rack space etc., in accordance to the equipment proposed at Data Centre Lucknow and Bengaluru, as 1PB Storage at these Data Centres are to be installed within the Smart Rack.

Sr. No.	Specifications
1	This specification covers intelligent integrated/inbuilt infrastructure, standalone system design, engineering, manufacture, assembly, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for proposed Data Centre to be installed at Command Centre, as detailed in the specification, complete with all accessories required for efficient and trouble free operations
2	Modular and scalable design for power and cooling : All the components used to design the system should be redundant and in the Events of failure the components can be maintained easily. All the components of the infrastructure should be such that it can be easily dismantled and Relocated to different location.
3	Intelligent Integrated Infrastructure with inbuilt hot and cold aisle containment of **7 usable racks** should cater to IT load up to 55 KW
4	Intelligent Integrated Infrastructure essentially should include internal redundant or backup power supplies, environmental controls (Precision Air Conditioning (PAC), Fire Suppression, Smoke Detection, Water Leak Detection and Humidity Sensors), and Security Devices. Critical systems like UPS should have N+N redundant topology, and PAC should have N+1 redundant topology. Environmental monitoring shall be done from IP based software. All these components should be designed and prefabricated by the same OEM.
5	The detail specifications of the intelligent integrated/inbuilt infrastructure, standalone system shall be in adherence to standard Data Centre guidelines thus shall be composed of multiple active power and cooling distribution paths, but only one path active. Shall have redundant components to avoid single point of failure.
6	**The Intelligent integrated Infrastructure shall have following components:-**
6.1	**In-Row closed loop Air-Conditioning**
6.1.1	Data center server and network racks should be equipped with In-row Variable / digital scroll cooling units to provide closed loop precision cooling system which should be able to cool the equipment's uniformly right from 1st U to 42nd U of Rack
6.1.2	Precision Air Cooling should be should be of 55KW capacity N+1 topology.
	Precision Air Conditioner should have following Features:
	□ Cooling System should be DX (Variable) type in N+1 Topology
	□ Inbuilt Heater and Humidifier to cater IT load up to 55 KVA
	□ Outdoor Unit
6.2	**UPS System**
6.2.1	Each UPS should be 60KVA Modular UPS with N+1 module level redundancy, rack mountable with pf up to 0.9 and efficiency at least 92-94%. Other features of UPS system are as follows:
	□ True On-line UPS with Widest input range (228V-478V)
	□ Double conversion and IGBT technology : Full IGBT Rectifier /Battery Charger and IGBT based Inverter
	□ Battery backup of 30 minutes (Minimum 2 strings of batteries to avoid single bank failure)

	Archiecture: Modular, scalable, redundant based minimum rating of Power Modules 20KVA. Each rated module should be further splited into three granular modules of equal capacity
6.3	**Power Distribution**
6.3.1	Standard Rack metered IP PDU (Vertical) - with 16 sockets (12 IEC C13 & 4 IEC C19)-02 Nos. for each Rack with 2.5 mtr. power chord (each rack should have two PDU's).
6.4	**Main Electrical Panel and Cabling**
6.4.1	DB panel should be mounted on to utility rack only with all internal cabling integrated into the same. Essential MCB/MCCB should be provided with electrical system. The panel must have protection against fire hazards and should have fire detection and NOVEC 1230 Gas based suppression system.
6.5	**Fire Detection and Suppression**
6.5.1	Fire detection and suppression system : Fire detection and suppression system should be mounted in panel adjacent to Smart Racks to avoid consumption of any usable U space an In-rack built-in feature of solution. It should have Fire alarm and fire suppression unit and the fire suppression agent should be NOVEC 1230 Gas as per NFPA 2001 guidelines
6.6	Blanking Panel: 30%
6.7	**Environmental Controls**
6.7.1	Each set of intelligent rack should include basic environmental controls: □ Smoke Detector □ Water Leak Detection system □ Temperature/ Humidity Sensor □ Door Sensor □ Alarm beacon
6.8	**U Space**
6.8.1	Intelligent racks should have Minimum 7 x 42 U Rack usable space available for IT equipment's and network equipment, with UPS and battery externally placed.
6.8.2	**Racks**
6.8.3	Insulated 42 U Racks Width – 600mm Depth- 1000 mm
6.90	**Other features:**
6.9.1	The Intelligent integrated infrastructure would provide much functionality and some of the key functionalities are - Integrated UPS, Cold aisle & hot aisle contained, Integrated Fire system, insulation, remote Management system from single OEM for seamless integration and better after sales support.
6.9.2	Intelligent integrated infrastructure would have provision to add an extra rack in future. It should be flexible, adaptable, controllable infrastructure.
6.9.3	Biometric access control system provided should be controlled by access control panel
6.10	***Monitoring -***

6.10.1	Supply and installation of monitoring system with Sensors & notification system. The system shall continuously collects critical information from network connected devices such as UPS system, Cooling Units , temperature & humidity sensors, Door sensors, Water Leak sensor and other dry contact monitoring. Beacon & Buzzer-Sound and Flash Led Alarm. Based on pre-set parameters, automated email alerts are sent to the intended recipients
6.10.2	Intelligent Rack environment remote monitoring
6.10.3	Intelligent racks should have IP based monitoring facility of all the passive parameters inside racks. All racks will be monitored with single window console
6.10.4	Capable for Email Alerts
6.10.5	System required for monitoring all parameter – Temp, Humidity, Door access, Smoke, WLD, UPS, Rack power on single window.
6.10.6	Modbus 485 Communications
6.10.7	SNMP Communication
	Single window for monitoring all sensors
	Temperature & Humidity Sensor
	Data and logs of historical information of alarms and notification
	Door opening sensor
	Water leak detection sensor
	Smoke detection sensor

ORC

Annexure – C29: Server Rack 42U

Sr No	Specification
1	Adjustable 19” equipment mounting verticals provide the better mounting flexibility maximizing the usable mounting space
2	Depth adjustable mounting slots
3	Standard Color : Black or Grey
4	Top and bottom Panel with ventilation and cable entry facility
5	Provision to mount the cooling fans on the top panel
6	Powder coated finish with pretreatment process meeting all industry standards
7	Grounding and Bonding Options
8	100% assured compatibility with all equipment conforming to DIN 41494. General industrial standard for equipment
9	42U Closed Rack / Width 800mm / Depth 1000mm
10	Construction : Welded OR CKD (Knock Down)
11	Front Door : Lockable Toughened Glass Door
12	Rear Door : Steel Door
13	Basic Frame : Steel
14	Equipment Mounting : DIN Standard 10mm Sq. Slots / Direct M6 Tap
15	Mounting Angle : 19” Mounting angles made of formed steel
16	Standard Finish : Powder Coated
17	Top and Bottom Cover : Welded to Frame, Vented and Field Cable entry exit cut outs
18	Mounting Option : Castor wheels (Front 2 wheels with Break and rear without break) Or Leveler’s Or Base plinth
19	Power Input: Should be compatible with single phase, 60Amp industrial socket.
20	Accessories: Doors & Side Panels, Power Distribution Units, Cable Manager, 4 * Fans and Fan Modules, Jacking Feet, 5 * Mounting Hardware, Vertical Power strip with 12 nos of 5/15A sockets (high end).

Annexure – C30: Application Delivery Controller With Global Load Balancing

Sr No	Specifications
1	Required Interfaces 8 x 10 GbE SR SFP+ and option for additional 2 x 40GbE QSFP ports for future
	SSL and Compression throughput of 20Gbps
	Layer 4 Request per second: 10 Million
	Layer 7 requests per second: 1.5 Million RPS
	Should provide Layer-7 throughput minimum 30 Gbps.
	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1
2	The SLB should support the below metrics:
	— Cookie Persistence ,
	— Observed and Predictive or Hash IP,
	— Least Connections, Users, Bandwidth
	— SNMP based like - CPU/ Memory/ Network utilization
3	The proposed ADC should have Virtualization feature that virtualizes the Device resources— including CPU, memory, network, and acceleration resources.
	Proposed device should support minimum 5 Virtual Instances.
4	Should have Global Server load Balancing with DNS-Sec
	Should support following DNS functionalities: A, AAAA, AXFR, CNAME, IXFR, MX, NS, PTR, SOA, SRV, TXT.
	Should support server side web compression and proximity based Global Load Balancing.
5	Should support following Web Application Performance Optimization features:
	a) Simplifying large, complex web pages.
	b) Caching, Compression
	c) Accelerate entire web transaction
6	Should support user-written scripts, that provide flexibility to control application flows
7	Should support Active-Hot Standby, Active-Backup redundancy with maintaining session state.
	SLB Device should be accessed through the below:
	CLI, SNMP, REST API, Web Based Management
8	Offered solution should be EAL or NDPP (Network Device Protection Profile) certified under Common Criteria Program for security related functions or ICSA Lab certified.

Annexure – C31: DDOS Protection

Sr No	Specifications
1	Offered solution should be EAL or NDPP (Network Device Protection Profile) certified under Common Criteria Program for security related functions.
2	DDoS mitigation solution should be a dedicated appliance (not a part of Router, UTM, Application Delivery Controller) with minimum 20 Gbps of DDoS Mitigation Throughput.
3	Support DoS Flood Attack Prevention Rate: Minimum 25 Mpps.
	Should have the capability to handle minimum 20 Million Legitimate TCP concurrent Connections.
	Inspection Ports required: 8 x 10G SFP+ (SR Populated), support for 2 x 40Gbps ports for future.
	Security Protections:
4	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against IoT botnet threats, including Water Torture, Burst and Randomized attacks. Should provide DNS based DDoS attack protection for individual record type like A, AAAA, CNAME, PTR, MX, NS
5	POSITIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic
6	ZERO DAY ATTACK PROTECTION should be provided by behavior-based protection with automatic signature creation against unknown, zero-day DDoS attacks.
7	CUSTOM TAILORED HARDWARE must be proposed using dedicated DoS Mitigation platform which off-loads high volume attacks, inspecting without impacting user experience.
	Behavioral DoS Protection
8	Behavioral DoS (Behavioral Denial of Service) Protection 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.
9	Network-flood protection should include:
	• TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood
	• UDP flood
	• ICMP flood
	• IGMP flood
10	OEM has to provision for knowledgeable and specialized security experts (on call - on remote), who provide 24x7 (SLA defined), Real Time Professional Services/ TAC/ SOC services for the network facing denial-of-service (DoS) attack in order to restore network and service operational status.
11	The proposed solution shall meet following DNS protection functionality:
	• DNS DDoS mitigation
	• DNS Protocol inspection and validation
	• Should support DNSSEC
	• DNS DDoS threshold alerting
	• DNS query limit
	• DNS NX-Domain attack protection
	• DNS TCP active authentication
12	Centralized Monitoring and Historical Reporting solution should be provided from Day 1

Annexure – C32: Network Intrusion Prevention Specifications (NIPS)

S.No	Requirement
1	The IPS should be a Dedicated purpose built hardware, NOT a part of Firewall module or UTM solution
2	The IPS should have Real World Throughput of 20 Gbps, scalable upto 30 Gbps without hardware change. And should have SSL throughput of 10Gbps scalable to 15 Gbps.
3	NIPS should be from different OEM as of Networking (Router-Switch), DDOS, WAF & Firewall proposed in this case.
4	Solution should provide Intrusion Prevention System, Anti Malware, Application control capabilities. Should support SSL inspection either integrated or with external device.
5	Maximum concurrent connections should be 10 Million. And IPS should employ full seven-layer protocol analysis of over 100 internet protocols and data file format.
6	**Inspection Ports:** 4-port 1 GigE with fail-open, 16-port 10 GigE SFP+ SR Optical with fail-open. Should support 2 x 40G for future use.
7	**Should support following Deployment Modes:** In-line; SPAN Port Monitoring
8	**Block Actions :** Drop packet, TCP Reset, Quarantine, Alert.
9	**The proposed solution must support the following Network-wide protections:**
A	**DoS Protection**—Protection against Volume-based Denial-of-Service attacks including SYN Floods, TCP Floods, UDP floods, ICMP and Application level flood.
B	**DNS Protection**—Protection against DNS query floods.
C	**Signature-based Protection**—Protection against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS. OEM should have its own threat intelligence database, not dependent on open source
D	**Self- learning capability —** Should have capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network
E	**Control traffic based on geographical locations** – Should be able to block traffic coming or going to a particular country. Provision should be there to allow specific IPs for any blocked country
F	**Black List rules and White List rules--** Block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.
G	**Malware Protection** : • The solution should support malware protection by performing file reputation analysis of malicious files. • Solution is required to scan all all types of office files including PDF, MS Office, Star office, etc..
10	**High Availability :** High Availability : Solution should provide failover among devices for all components and should be completely automatic without any sort of manual intervention. The solution must support Active-Failover and Active-Active architecture and high availability options for redundancy with/ without using any third party or additional software or hardware
11	**Reporting** : The proposed solution must have historical security reporting solution, which provides the following:• Customizable dashboards, reports, and notifications• Centralized Management Solution should have capability of high availability at site level for enabling DR deployment
12	OEM should have support centre / TAC based out of India.
13	The solution should be proposed with Premium Support with single point of contact directly from OEM for all post-sales issues. The same should be certified by OEM with relevant documents. OEM should provide quarterly health review of the solution.
14	IPv6 support is required. NIPS is expected to detect and block attacks in IPv6 traffic

Annexure – C33: Captive Security Operation Centre (SOC)

Annexure – C33(a): Incident Response services from Security OEM

As a part of SOC solution Bidder shall propose the Incident Response services from Global security OEM who has been providing such services. As a part this services bidder should include:

- One-time Incident Response Plan development services from OEM after the commencement of SOC
- Annual Advanced Threat Hunting service once in a year
- Minimum 10 Man Days of OEM IR services/ year on demand
- Should also submit the change request format to ORGI for their approvals for additional Man days if required on demand for OEM advance IR services

The proposed Advances IR services from Security OEM should provide minimum following Characteristics::

Sr No	Minimum Feature Requirements
1	OEM must provide advise on full scope of cyber security incident response (IR) retainer service
	• Identification
	• Containment
	• Eradication and Recovery
	• Malware analysis and reverse engineering
	• Reporting
	• Incident response readiness assessment
	• Incident response plan development
	• Incident response training
	• Advanced threat hunting
	• Cyber security assessment
2	OEM must provide following activities as part of Advanced Threat Hunting once a year: • Project Planning • Understand requirements and define scope • Identify ingress and egress points for traffic monitoring • Leverage End-point Agents • Leverage Network Forensics Platform • Data Capture & Gathering • Perform End-point Sweeps and gather data for analysis • Perform Full packet network capture analysis over a defined time interval • Gather logs and alerts (NIPS, HIPS, Firewall, Antivus, etc.) • Acquire evidence using threat hunting tool. • Detection & Analysis • Perform forensic analysis on threat hunting tool output • Use Adversary Intel, OSINT and Indicators of Compromise (IOC) to look for attack patterns • Reporting • Detailed Network hunting report • Detailed End-point hunting report • Management Presentation • Recommendations to improve security posture
3	OEM must have produced research papers and published vulnerabilities. OEM should have minimum 10 resources Incident Response professionals with average of minimum 5 year in-field active investigation experience.
4	OEM must have at least 10 cyber incident response experts that hold at least three (3) of the following qualifications: - GREM, GCFE, GCFA, CEH, GCIH, GCIA, CCFE, CPT, CREA
5	This declaration has to be submitted on OEM letter head with name and qualification of such resources.
6	OEM must help with Incident Response Plan Development which will help in following ways:
7	An Incident Response Plan should foster a continuous improvement process that leverages lessons learned from past incidents to improve overall security effectiveness.

8	An Incident Response Plan documents the processes and procedures, roles and responsibilities of various stakeholders, and communications flows and notifications procedures that are critical in timely recovery from security incidents.
9	The incident response practice should have a closed loop feedback into the intelligence program
10	Annual Advanced Threat Hunting service should use and integrate with the Full Packet Capture & Network Forensic solution as asked in SIEM in this RFP to provide the necessary report to highlight presence (in case presence is there) of compromises and threat activities previously un-identified in customer environment.
11	OEM must confirm that they have single tier of Analysts & customer will be consistently provided same or equally qualified analysts for all the activities.
12	OEM must perform Advanced Threat Hunting once in a year at ORGI premise with the above mentioned tools.
13	OEM must help in building detailed Incident Response Plan once in a year
14	OEM must have fully functional Global Security Operation Center.
15	OEM must have SANS certified engineers to undertake proactive Threat hunting. These Engineers must have minimum 5 years of industry experience in IR.
16	One-time Incident Response Plan development services: An Incident Response Plan Assessment report should comprise in-depth assessment of ORGI's information security incident response plan. OEM should work with ORGI to determine current and future needs and examine how the incident response plan currently operates from a strategic, operational and tactical viewpoint. An incident response plan assessment should be performed using a series of questionnaires, workshops and interviews. Vendor should provide an assessment snapshot with recommended actions presented at the end of the activity.
18	Annual Advanced Threat Hunting service OEM must search ORGI's network to attempt to uncover the presence of compromises (a compromise assessment) and threat activity previously unidentified in ORGI's environment. Vendor must use hunting methodology and ORGI deployed forensic technologies to search networks and identify the presence of possible threats ranging from undetected malware to full advanced persistent threat activity.

Annexure – C33(b): Threat Intelligence Feed from Global Security Vendor

As a part of SOC solution Bidder shall propose Threat Intelligence Feed from Global security OEM with following minimum characteristics. The Threat intelligence platform should provide data feeds that integrate into a SIEM, a customizable research application that can be customized for use by the organization.

S.No.	Minimum Features / Specifications
1	Vendor Threat Intelligence should have intelligence build using monitoring of following minimum events: a. More than 100K sensors monitoring networks b. More than 1 billion emails per day c. More than 10 million web requests a day d. Must monitor globally over 10 million products and services e. Intel collection in more than 20 languages. f. Intel should include more than 50,000 IOC's in a month g. Must monitor globally not be limited to only English-speaking sources, also be collected and interpreted from non-English source like Chinese, Russian, Urdu, Ukrainian, Arabic, Persian, Spanish etc.
2	Vendor must provide Advanced IP Reputation.
3	"Vendor must refresh the data feed when new feed is available, minimum frequency every 24 hours.
4	Vendor must province following attributes as part of data-feeds based on the availability: a. IP Domain, Hostility, Reputation, Confidence, Behavior, Consecutive Days, Listing over a 90 day window, Geo-location Attributes, Industry Attributes, Ownership Attributes, Registration Attributes, Attack Behavior Details, Malware Behavior Details, Phishing Behavior Details, Fraud Behavior Details, Bot Behavior Details, CnCBehavior Details, Spam Behavior Details
5	Vendor must provide the data feed in any three formats out of XML, CSV, CEF, OpenIOC, STIX formats and should be compatible with the SIEM.
6	Vendor must provide perl/ python/ bash scripts/ API in order to download and consume the data feeds.
7	Vendor must provide additional information in IOCs wherever requested.
8	Threat Intelligence feed OEM should have experience of at least 5 years of providing such proposed threat intelligence. Confirmation required on OEM letter head.
9	The asked Threat Intelligence feed has to be unique. This has to be from a different OEM and not the same as of SIEM OEM. Threat intelligence should integrate with the SIEM
10	Threat Intelligence should give reference of minimum two customers in India to whom such satisfactory threat intelligence services are being provided. Confirmation required with name/address/ contact details of such customers in India

Annexure – C33(c): Onsite Cyber Security Team (Skilled Manpower)

MSI should quote for OEM Certified team of Cyber Security Experts to provide coverage for rotational shift to perform the following activities

1. Daily Operational Checklists for Log analysis, alert analysis, log source coverage and escalation activities are in order.
2. Investigate suspicious security events.
3. First level incident response for confirmed incidents received from monitoring and notification team.
4. Verifying that security feeds are correct and confirm that all monitoring and activity-based reports are completed
5. Analyze use cases; reduce false positives and create new use cases
6. Analyze the threat intelligence feeds, process and provide actionable input

The Responsibilities and Skill matrix is mentioned below, mentioned number of resources are minimum, MSI has to decide on the required number of resources depending upon the SLA:

S.No.	Resource	Responsibility	Skill Set
1	Senior Cyber expert & Lead- minimum 1 Nos.	• SIEM use case development • Use case configuration • Response / Workflow configuration • Incident Response coordination • Recommendation • Reporting • Metric Management	1. Over 7 years of experience in consulting, deployment of SIEM, use cases and incident response procedures and recommendations. 2. Experience in drafting processes, procedures and operational parameters for SOC 3. Engineering Graduate 4. Good logical reasoning and analytical skill 5. Good communication skill 6. One security certification and or SIEM certification.
2	Cyber expert – 3 in Nos.	• SIEM rule base management • Detecting suspicious events and incidents • Weekly analysis report for true positive, false positive, common incidents, MTTD etc.	1. Over 4 years of experience in Security log analysis and use cases (alert and multi device correlation) 2. SIEM knowledge and product certification 3. Engineering Graduate 4. Excellent analytical and logical analysis skill 5. Knowledge base management 6. Incident management and point tool integration experience

Annexure – C34: Router for 3 Main Data Centres

Sr No	Specification
1	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT), capability. The router shall also support In-band and out-band management, Software rollback feature, Graceful Restart, non-stop routing for OSPF, BGP, LDP, MP-BGP etc. The platform shall have modular software that shall run service & features as processes having full isolation from each other.
2	The router should have 8xSFP+ interfaces with 4 SR (10Gbps) & 4 Sx (1Gbps) Transceivers and should support 2x 40G interfaces for future
3	The routing aggregate throughput should be at least 25 Gbps which can scale up to 50 Gbps to meet future requirement without changing the hardware.
4	The proposed router shall support minimum 10 VRFs
5	The router shall support the IPv4 and IPv6 DUAL-stack in hardware and software.
6	The router shall support minimum 3 million IPv4 & IPv6 Routes with 8,000 Multicast Routes
7	Shall have Multicast routes & IGMP groups.
8	The router shall have RIPv1, RIPv2, RIPng, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation).
9	The router should have support for 4,000 IPSEC tunnels and 1000 tunnels of GRE.
10	The router shall support QoS policy in the router shall support Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QOS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non- congestion scenario.
11	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP
12	The router shall support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT). The router shall support NAT6 to 4 function. Router shall support at least 2 million NAT sessions
13	The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc.) and Port Range etc.

Annexure – C35: Firewall with Virtualization

Sr No	Specifications
1	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems.
2	Firewall appliance should have at least 8 x 1GE SFP, 8 x 10G SFP+ SR interfaces and 2 x 40G SR interfaces fully populated.
3	Firewall should support minimum 80 Gbps Throughput in both IPv4 and IPv6.
4	Firewal should support minimum 20Gbps of VPN throughput.
5	Firewall should support minimum 10,000 site-to-site & client to site VPN Tunnels.
6	Firewall should support minimum 10,000 concurrent SSL VPN users.
7	Firewall should support minimum 500,000 new sessions per second.
8	The Firewall solution should support NAT64, DNS64 & DHCPv6
9	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.
10	The proposed system should have integrated Traffic Shaping/ rate limiting functionality.
11	Offered product family should be EAL or NDPP or ICSA certified.
12	The device shall utilize inbuilt hardware/ Software VPN acceleration for IPSEC (DES, 3DES, AES) encryption/ decryption & SSL encryption/ decryption OEM specific
13	The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.
14	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided and it should be scalable to 200 Virtual Firewalls in future.
15	The proposed system shall have the ability to detect, log and take action against network traffic based on over 4000 application signatures
16	The application signatures shall be manual or automatically updated
17	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component
18	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.
19	High Availability Configurations should support Active/Active and Active/ Passive
20	Logs and Report
21	Should have 4 TB of Hard Drive Capacity for logging and reporting if not please quote external appliance
22	Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination IP, user details etc

Annexure – C36: Network Access Control (NAC)

S.No	Specifications
1	**General Requirements**
	Provide an easy-to-use BYOD ready granular secure access control solution that is context aware, identity enabled, location and device based. The proposed solution must combine Authentication, Authorization, and Accounting (AAA); Posture; Profiling; and Guest Access management services on to a single platform with a minimum endpoint footprint and supports the ability to be managed from a single management console.
2	**Architecture**
	The proposed NAC solution must be vendor agnostic solution to work in heterogenous network and it must support centralized deployment and Distributed deployment
3	**Profiling / Visibility**
	The proposed NAC solution should be able to detect both new and existing endpoints and categorizes them based upon the type of endpoint (Ex: Windows, Printer, Network Device, IP Camera, Android, iPad,etc). It must provide flexible filtering capabilities to sort out device information based on differen attributes (e.g MAC address, Manufacturer name, hostname, IP address, etc.).
	The proposed NAC solution must support Profiling via Passive and Active collectors which includes SNMP, HCP fingerprinting, HTTP-agent, NMAP, WMI, SSH etc.
4	**Behavioral Analytics**
	The proposed NAC solution should be able to analyzes user or device behavior using the following methods: 1) Adaptive Authentication 2) Anomalous Traffic from IoT devices 3) Potential Malware Detection
5	**Access control from Complete Unmanaged environment**
	Access control from Complete Managed environment : The solution should be able to provide authorized access in an environment with managed switches. The solution should be able to do compliance check in a managed environment.
6	**Role-based Access / Enforcement**
	The proposed NAC solution shall include the following key components: a) RADIUS server; b) NAC client agents; c) Policy Manager; d) Enforcement Manager; e) Integration Interfaces; f) Pre- and Post-admission control for network access; g) Agentless based access with posture check for domain machines
7	The proposed NAC solution must be capable of supporting 802.1X and SNMP enforcement for managed endpoints and MAC Authentication Bypass (MAB) for unmanaged endpoints like (printer, IP camera, etc.). It should support Dynamic ACL and dynamic VLAN enforcement through SNMP.
8	The proposed NAC solution should integrate with multivendor Switches and Wireless Controllers to support enforcement actions such as Switch port Block Assign to VLAN and Port ACL on non-compliant / unknown users.
9	The proposed NAC solution must enforce security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention. Once the user's machine is remediated, the user's machine shall be redirected automatically to the assigned network segment for access to the Site resources and the services that they are granted access.
10	The proposed NAC solution should be able to perform endpoint posture verification without agent, dissolvable agent or any install on the endpoint
11	The proposed NAC solution must be able to remotely install agents to corporate hosts without end-user interaction
12	**Clients**
	The proposed NAC solution must support automated provisioning and deployment clients remotely. It must support a Unified NAC client shall support both NAC and VPN functionality.
	The proposed NAC solution should support agent, agentless and disolvable agent for Authentication and compliance check

13	**Customized Device Templates**
	The proposed NAC solution should allow administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network
14	**Authentication Protocols**
	The proposed NAC solution must support the following authenticating protocols: Supports PAP, MS-CHAP, MS-CHAP-V2, EAP-MD5-Challenge, EAP-MS-CHAP-V2 (EAP)-MD5 Protected EAP (PEAP) EAP-Transport Layer Security (TLS) EAP Generic Token Card (EAP-GTC) EAP State of Health (EAP-SOH)
	The proposed solution should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases: a)Local Databased on the NAC device b)Radius c)Active Directory d)LDAP e)TOTP f)SAML g)SQL h)Site Minder i)ACE/RSA j)NIS k)Certificate Server
15	**Host Checking**
	The proposed solution should support automated and manual remediation methods for killing process, setting registry keys, starting antivirus, update anti-virus, starting windows services, starting windows updates, disabling/enabling USB Ports, checking custom process, checking custom ports, patch management control. It should have a GUI based console to support administrators/users to perform such remediation methods manually, automatically and in scheduled manner.
16	**Guest Management**
	The proposed NAC solution must provide complete guest lifecycle management by allowing non-IT employees to provide controlled access to guests and consultant reducing the IT workload
	Guest management portal shall support self-onboarding and Sponsor based guest access control for Guest/Contractor devices.
	Guest registration shall support multiple credential notification methods (SMS, Email, webpage, etc.)
17	**Eco-system Integrations**
	The proposed NAC solution should integrate with next-generation Firewalls (Palo Alto Networks, Fortinet, Checkpoint, Juniper SRX, Netscreen, etc.). It should also integrate with other security solutions like MDM, ATP, SIEM, Identity providers (Duo, RSA, etc.), WLCs.
18	**Redundancy Support**
	Support 1+1 High Availability Configuration with options for Hot Standy-by and Active/Active redundancy
19	**Monitoring and Reporting**
	Support built-in monitoring , reporting , and troubleshooting console to assist helpdesk operators and administrators streamline operations. NAC GUI should support Dashboard with contextual information (compliance, number of users, devices, etc.), Wizards for ease of configuration and historical data on contextual information. It must provide device reports in CSV, Tab Delimeter and PDF formats.
20	**Centralized Management System**
	The network access control policies should be managed and have the capability to be pushed down configuration centrally. Centralized management system should provide a single-pane of glass view for all endpoint information
21	**Platform Hardware**

	The proposed solution must be a purpose built 1U 19" rack-mountable appliance with 8 GB RAM and 500 Gb Local storage capacity. It should support at least 9000 concurrent NAC users/devices in a single box and support the ability to cluster up to atleast 4 boxes

ORGI

Annexure – C37: Antivirus for 18 DCC locations

Endpoint protection for Servers and workstations at 18 DCC locations:

Sr. No.	Specifications
1	Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation.
2	Solution should be offered on-premise.
3	Solution must have an option to raise support ticket from the management dashboard and must have global security news feed.
4	Solution should be Anti-Exploit, Anti-Ransomware and similar kind of attacks.
5	Solution must have the application control lets admin detect and block applications that are not suitable for use in the office.
6	Proposed solution should show the alert description along with User & Device.
7	Solution must support Runtime Behaviour Analysis / HIPS.
8	Solution must offer the Device Control/Peripheral control, with the Option of Read Only, Allow, Block access to the device.
9	Solution should have the option to block the website on the category basis and detect the C&C communications
10	Solution should have the data loss prevention functionality.
11	Solution should provide the Root Cause Analysis/threat cases powered by Deep learning
12	Solution must have the Threat cases that generate Root Cause Analysis that provides the who, what, when, where, and how of a given attack, allowing IT the ability to constantly improve upon their security posture

Annexure – C38: Situational Awareness & Analytics

Sr No	Specifications
1	The solution should provide continuous security monitoring & comprehensive network visibility into network traffic activity, applications, assets and security risks - using high-speed full packet capture technology.
2	It should support a scalable modular architecture that comprise of presentation layer, data acquisition & enrichment layer, a streaming & automation layer and, a data-repository layer.
3	The solution should support minimum of 10Gbps full-duplex sustained capture performance with support for multiple ingress interfaces for capturing from various sources in the network. Appliance should have 4 x 10G SR interfaces. Solution should support Network traffic capture using network tap, a SPAN port, and/or port mirror.
4	The solution should be provisioned with storage to support information-element lookups for 7-days traffic captured by the system. The solution should integrate with direct-attached and network-attached storage to increase capacity. It should be possible to back-up and restore metadata.
5	The solution should integrate with SIEM or log management tools for sharing of network metadata in real time and, alerts as they happen.
6	The solution should support importing of PCAP and other raw packet capture format files for analysis. The solution should not hold or stop live capture to process imported captures.
7	The solution should generate and represent metadata pertaining to L2 - L7 and, enrichment processes such as static correlation, dynamic analysis, or, analytics outcome, etc. in a single repository.
8	The solution should facilitate a search-driven data discovery of metadata and captured content for incident analysis.
9	The solution should allow chronological retracing of activities pertaining to a a security event or an incident.
10	The solution should be capable of reconstructing sessions and allow retrieval/ investigation of data accessed and transmitted while recording full packet captures. It should be possible for a user to extract content-information in metadata pertaining to web, mail, file-transfer, audio/video calls, encryption ciphers, identities, etc.
11	The solution should support generation of a link-graph to represent network communications and, allow for proactive threat-hunting or investigations to be carried out using the visual link analysis.
12	The solution should be able to capture all network traffic across its monitoring interfaces and process in real-time to detect abnormal network behavior using unsupervised machine learning algorithms on all sessions. It should be capable of matching network activities to proactive rules for detection of threats or insider misconduct. The Machine Learning capability should be OEM's own work and not sourced from a third-party.
13	The solution should permit creation of static rules that apply to metadata or the content or both. The solution should also allow creation of complex behavior based rules that detect anomalous activity based on an event happening or repeating itself in a defined timeframe. It should also be possible to write rules to detect unique activities in a given timeframe.
15	The solution must be able to detect suspicious communication channels, services or, applications not running over their standard designated ports (i.e. HTTP application not using TCP port 80).
16	The solution should be capable of performing analytics on encrypted communication without the need of deploying decryption technology or man-in-the-middle solution. It should be possible to perform analytics on non standard ciphers and, encrypted traffic including SSL, TLS, IPSec, SSH, SMTPS, IMAPS, etc.
17	Situational Awareness and Analytics should be available as a separate stand-alone solution and not as a component of a larger portfolio of any other Application Monitoring Platform.
18	The solution should offer a stand-alone discovery console for the administrator to search through the captured data-set.

19	The solution should perform Deep Packet and Payload inspection to dynamically detect protocols and applications. It should support detection of over 2,000 protocols and applications in network traffic. The DPI should detect applications in tunneled or encrypted traffic. The solution should enrich communication information with correlations such as names resolution, geolocation, device, platform and, user identities without the need for installing endpoint agents. The Deep Packet & Payload Inspection capability should be included as a part of the Packet Capture engine. It should not require addition of licenses or another product to be deployed.
20	It should be possible to integrate output from the solution into another big data repository by enabling real-time streaming delivery of metadata to an external, third-party receiver.
21	The solution should support a web based user interface with ability to obtain attack context using visual analytics, be able to manually detect anomalous events by proactive tools including (but not limited to) applications such as network graphs, event timelines, free text search, drill-down, etc. The UI should also allow the solution to retrospectively analyze past events.
22	The solution should support exporting information from UI visualizations in real-time so that the output can be integrated with offline analytics tools such as Microsoft Excel.
23	It should be possible to orchestrate a response by extracting actionable intelligence into a template that can be shared with other security tools and processes.
24	The solution should not send any metadata or information outside of the network where it is deployed. It should be possible to perform threat/ risk detection without connecting the system to the Internet.
25	The OEM should have Product R&D and Technical Assistance Centre based in India.
26	The solution must support replay of packets and metadata both in real time to third party solutions hosted on other systems.
27	The solution should integrate with map server to display communication patterns, applications on world-map and allow for search/filtering based on geolocation and should support irregular polygonal geofencing filters.
28	End user should be able to contact the OEM support directly via web and phone. The support should be based out of India.
29	The solution should be proposed with Premium Support directly from the OEM for all post-sales issues. The same should be certified by OEM with relevant documents. OEM should provide quarterly health review of the solution.

Annexure – C39: Manufacturer Authorization Format

Ref : Date:

To,
Joint Director (HO),
Office of Registrar General, India ,
NDCC-II, Jai Singh Road,
New Delhi – 110001

Sub : Manufacturer Authorization for Tender No.

Sir,

We, **<OEM/ Manufacturer name>** having our registered office at **<OEM / Manufacturer address>,** are an established and reputed manufacturer of **<components proposed in bid>**. We have presence in India for more than 5 years.

We confirm that **<Bidder Name>** having its registered office at **<Bidder Address>** is our authorized partner for following Hardware, Software components proposed in this tender.

We authorize them to quote for our equipment's **<Components proposed in tender>** in the abovementioned tender. Our full support is extended to them in all respects for supply, warranty and maintenance of our products. We also ensure to provide the service support for the supplied equipment's for a period of 5 years from the date of installation of the equipment's as per tender terms. We also undertake that in case of default in execution of this tender for our equipment's by the **<Bidder Name>,** the **<OEM/ Company Name>** will take all necessary steps for successful execution of this project as per tender requirements.

We confirm that support for offered components will be available for 8 years from date of Acceptance."

Since the latest solution is being procured with a 5 years warranty from the date of acceptance. Therefore, it is ensured that the support for the same will be available for additional three years, after the expiry of warranty period.

Thanking You

For **<OEM/ Manufacturer name>**
<(Authorized Signatory)> Name
<OEM Stamp>

Annexure – C40: Format for Declaration by the Bidder for not being Black-listed

(To be submitted on the Letterhead of the Bidder)

Dear Sir,

We confirm that our Company **<name of company>** as on date of submission of the proposal is not been blacklisted by any Private/Central /State Government/PSU or any other Organization and agencies in India for corrupt, fraudulent or any other unethical business practices.

Sincerely,

Name & Designation of the Authorized Signatory
Designation: Country Head/ Legal Head

ORGI

Annexure – C41: BOM-HW (For Technical Bid)

The BOM (Bill of Material) in technical bid must be quoted separately for each technical annexure (C5 to C38) for single quantity of Workstation, server, storage, UPS, switches and printers etc. along with additional items (Resident Engineer) in following format without any price information.

S.No.	Product/ Hardware Item/ Resident Engineer	Description of Product/ Hardware with make and model (if any)	Quantity of Hardware/Resident Engineer	Bundled Quantity of Hardware
1	Item-1	Server Type-1	21	
2	Item-2	Server Type-2	54	
3	Item-3	Workstation	1,841	
4	Item-4	Mono Laser Printer	38	
5	Item-5	MFP Mono Printer	18	
6	Item-6	MFP Colour Printer	1	
7	Item-7	SAN Switch	8	
8	Item-8	Core Switch Type-1	6	
9	Item-9	Core Switch Type -2	18	
10	Item-10	Access Switch	66	
11	Item-11	Unified Storage (a) 1000 TB for NDC	3	
13	Item-13	Unified Storage for 18 DCC	18	
14	Item-14	Unified Storage (a) 1000 TB for NDC, ORGI		
15	Item-15	Unified Storage (b) 100 TB (Internal / External)	5	
18	Item-18	Unified Storage (c) 75 TB (Internal / External)	8	
19	Item-19	Unified Storage (8) 50 TB (Internal / External)	5	
20	Item-20	Backup Software (Licences per TB) 40% of VTL Capacity	240	
21	Item-21	Backup Appliance 200 TB	3	
22	Item-22	Backup Software Lic for TB	240	
23	Item-23	Backup Appliance 200TB	3	
24	Item-24	UPS 60 KVA	6	
25	Item-25	UPS 80 KVA	6	ONE
26	Item-26	UPS 40 KVA	6	
27	Item-27	Web Application Firewall	6	
28	Item-28	Database Activity Monitoring (DAM)	15	
29	Item-29	Patch Management	250	
30	Item-30	HIPS (Servers)	100	
31	Item-31	SIEM	1	
32	Item-32	End Point Protection and Remediation	250	
33	Item-33	Data Leak Prevention System (DLP)	250	
34	Item-34	Smart Rack for 2 DR	2	
35	Item-35	Server Rack 42 U	16	
36	Item-36	Server Load Balancer (ADC)	6	
37	Item-37	DDOS	6	
38	Item-38	Network Intrusion Prevention Specifications (NIPS)	6	
39	Item-39	Incident Response Services for SOC	1	
40	Item-40	Threat Intelligence Feed for SOC	1	
41	Item-41	On site Cyber Security Team for 60 months (security experts)	4	
42	Item-42	Router for 3 DC	12	
43	Item-43	Firewall with Virtualization	6	
44	Item-44	Network Access Control (NAC) Authorised Hosts	250	
45	Item-45	Anti Virus	1,966	
46	Item-46	Situational Awareness & Analytics	3	

47	Item-47	MS Windows Server Std latest edition 16 core license bundle (for 18 Data Capture Centre)	108	
48	Item-48	MS Windows Server Std latest edition 16 core license bundle (for 3 Datacentre)	105	
49	Item-49	MS Windows CALs	1,841	
50	Item-50	MY SQL Enterprise Server (Latest Edition) for 18 Data Capture Centres and 3 Data Centres	21	
51	Item-51	MS Office Professional Latest Version	41	
52	Item-52	Visual Studio Latest Enterprise Version	1	
53	Item-53	Resident Engineer for NDC & 2 DR sites (3 Shifts) (RE-1) for first 24 month	24	
54	Item-54	Resident Engineer for NDC & 2 DR sites (General Shift) (RE-1) for 36 months, After 24 months mentioned in Item-49(a)	12	
55	Item-55	Resident Engineer for DCCs (RE-2) for 60 months	19	
56	Item-56	Virtuliazation Software for Data Center Server	9	
57	Item-57	Link Load Balancer	6	

ORGI

Annexure - D2: PRICE SCHEDULE

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

Sl. No.	Item Description	Item Code / Make	Quantity	Units	FINAL RATE (WITH GST) of items with 5 yrs comprehensive warranty/ Resident Engineer with GST In Figures To be entered by the Bidder in Rs. P	TOTAL AMOUNT (WITH GST) of items with 5 yrs comprehensive warranty/ Resident Engineer With GST in Rs. P	TOTAL AMOUNT In Words
			A		B	C = A X B	
1	2	3	4	5	7	15	17
1.00	**System Integrator-hardware all kind of IT equipments/services/ manpower etc to be supplied**						
1.01	Virtuliazation Software for Data Center Server	Annexure-C2	9	nos			
1.02	Link Load Balancer	Annexure-C4	6	nos			
1.03	Server with Enclosure Type-1	Annexure-C5(a)	21	nos			
1.04	Server with Enclosure Type-2	Annexure-C5(b)	54	nos			
1.05	Workstation	Annexure-C6	1,841	nos			
1.06	Mono Laser Printer	Annexure-C7	38	nos			
1.07	MFP Mono Printer	Annexure-C8(a)	18	nos			
1.08	MFP Colour Printer	Annexure-C8(b)	1	nos			
1.09	SAN Switch	Annexure-C9	8	nos			
1.10	Core Switch Type-1	Annexure-C10	6	nos			
1.11	Core Switch Type -2	Annexure-C11	18	nos			
1.12	Access Switch	Annexure-C12	66	nos			
1.13	Unified Storage (a) 1000 TB for NDC, ORGI	Annexure-C13(a)	3	nos			
1.14	Unified Storage (b) 100 TB (Internal / External) for 5 DCC sites	Annexure-C13(b)	5	nos			
1.15	Unified Storage (c) 75 TB (Internal / External) for 8 DCC sites	Annexure-C13(c)	8	nos			
1.16	Unified Storage (d) 50 TB (Internal / External) for 5 DCC sites	Annexure-C13(d)	5	nos			
1.17	Backup Software (Licences per TB) 40% of VTL Capacity	Annexure-C14	240	nos			
1.18	Backup Appliance 200 TB	Annexure-C15(a)	3	nos			
1.19	UPS 60 KVA	Annexure-C16	6	nos			
1.20	UPS 80 KVA	Annexure-C17	6	nos			
1.21	UPS 40 KVA	Annexure-C20	6	nos			
1.22	Web Application Firewall	Annexure-C21	6	nos			
1.23	Database Activity Monitoring (DAM)	Annexure-C22	15	nos			
1.24	Patch Management	Annexure-C23	250	nos			
1.25	HIPS (Servers)	Annexure-C24	100	nos			
1.26	SIEM	Annexure-C25	1	nos			
1.27	End Point Protection and Remediation	Annexure-C26	250	nos			
1.28	Data Leak Prevention System (DLP)	Annexure-C27	250	nos			
1.29	Smart Rack for 2 DR	Annexure-C28	2	nos			
1.30	Server Rack 42 U	Annexure-C29	16	nos			
1.31	Server Load Balancer (ADC)	Annexure-C30	6	nos			

1.32	DDOS	Annexure-C31	6	nos			
1.33	Network Intrusion Prevention Specifications (NIPS)	Annexure-C32	6	nos			
1.34	Incident Response Services for SOC	Annexure-C33(a)	1	nos			
1.35	Threat Intelligence Feed for SOC	Annexure-C33(b)	1	nos			
1.36	On site Cyber Security Team for 60 months	Annexure-C33(c)	4	nos			
1.37	Router for 3 DC	Annexure-C34	12	nos			
1.38	Firewall with Virtualization	Annexure-C35	6	nos			
1.39	Network Access Control (NAC) Authorised Hosts	Annexure-C36	250	nos			
1.40	Anti Virus	Annexure-C37	1,966	nos			
1.41	Situational Awareness & Analytics	Annexure-C38	3	nos			
1.42	MS Windows server Std latest edition 16 core license bundle (for 18 Data Capture Centre)	Annexure-C1-Col5	108	nos			
1.43	MS Windows Server Std latest edition 16 core license bundle (for 3 Datacentre)	Annexure-C2-SNo-22	105	nos			
1.44	MS Windows CALs	Annexure-C1-Col9	1,841	nos			
1.45	MY SQL Enterprise Server (Latest Edition) for 18 Data Capture Centres & 3 DCs.	Annexure-C3-Col4	22	nos			
1.46	MS Office Professional 5 users server based Latest Version 18DCC an 3 DCs	Annexure-C3-Col3	41	nos			
1.47	Visual Studio Latest Enterprise Version	Annexure-C2-SNo-23	1	nos			
1.48	Per month Salary of Resident Engineer for NDC & 2 DR sites (3 Shifts) (RE-1) for first 24 months	No Annexure-1	24	nos			
1.49	Per month Salary of Resident Engineer for NDC & 2 DR sites (General Shift) (RE-1) for 36 months, After 24 months mentioned in Item 48(a)	No Annexure-2	12	nos			
1.50	Per month Salary of Resident Engineer for DCCs (RE-2) for 60 months	No Annexure-3	19	nos			
1.51	**Buy Back of old equipments From 18 Location as per annexure M**	**Buy Back of Hardware items from Annexure-D1**	**1**	nos			
Total in Figures							
Quoted Rate in Words							

Note:

1. **L1 Bidder will be selected on single Total Value as mentioned Total in Figures/ Quoted Rate in Words (BoQ/Price Schedule) above .**
2. The prices quoted should be including taxes/GST and should be inclusive of interface cables, Power Cables, related accessories, Documentations and Operating Manuals of the systems, five years on-site comprehensive warranty, packing, forwarding, freight, insurance (wherever applicable) and installation and services.
3. Bidder shall quote their competitive price online in the BoQ only.
4. Installation of all specified equipment to be done without any cost implication by the Service Engineer of concerned OEM only.
5. All Taxes and transportation cost for lifting the material for buyback items will be paid extra by the SI-H.

6. Single consolidated amount for Buy-Back value of all the old equipment as detailed in Annexure-M, has to be provided in against the S. No. 1.51 of BoQ (Annexure-D2).
7. Payment for Resident Engineers mentioned at S. No. 1.48, 1.49 and 1.50 of BoQ (Annexure-D2) will be calculated on monthly basis, but, will be paid on quarterly basis.
8. The quantity mentioned against each/any items of the Price Bid, may increase upto 30%, depending upon the requirement. Successful Bidder has to supply the increase quantity, on the same Terms & Conditions without change in specification/configuration.

ORGI

Annexure – L: List of Data Centers/Data Capture Centers

S. No.	Name of the Data Centre (DC)/ Data Capture Centre (DCC)
1	DCC, Chandigarh
2	DCC, Dehradun
3	DCC, R.K.Puram, Delhi
4	DCC, Jaipur
5	DC/DCC, Lucknow
6	DCC, Patna
7	DCC, Guwahati
8	DCC, Kolkatta
9	DCC, Ranchi
10	DCC, Bhubaneshwar
11	DCC, Raipur
12	DCC, Bhopal
13	DCC, Gandhinagar
14	DCC, Mumbai
15	DCC, Hyderabad
16	DC/DCC, Bengaluru
17	DCC, Thiruvanthapuram
18	DCC, Chennai
19	NDC, Shastri Park, Delhi

ORGI

Annexure – M: Data Centre-wise Numbers of Hardware items for Buy Back

Centre	Server	Workstation 1	Workstation 2	Workstation 3	Workstation 4	Mono Laser	MFD	Core Switch	HP 24 Procurve Switch	NAS 10 TB	NAS 100 TB	SAN 12 TB	UPS 60 KVA	UPS 40 KVA	UPS 20 KVA
Lucknow	3	98	16	2	48	3	1	1	5	1	0	2	1	0	0
Jaipur	2	67	12	2	24	2	1	1	3	1	0	1	0	1	0
Bhopal	2	92	16	2	25	2	1	1	4	1	0	2	0	1	0
Kolkata	2	84	12	2	32	2	1	1	4	1	0	2	0	1	0
Mumbai	3	104	18	2	50	3	1	1	4	1	0	2	0	1	0
Chandigarh	2	70	12	2	20	2	1	1	3	1	0	1	0	1	0
Bhubaneshwar	2	40	6	2	27	2	1	1	1	1	0	1	0	1	0
Bengaluru	2	59	9	2	29	2	1	1	2	1	0	1	0	1	0
Guwahati	2	46	4	2	22	1	1	1	2	1	0	1	0	1	0
Delhi (R K Puram)	3	118	20	2	0	3	1	1	5	1	0	2	1	0	0
Hyderabad	2	76	12	2	54	2	1	1	3	1	0	2	0	1	0
Chennai	3	68	12	2	56	2	1	1	3	1	1	2	0	1	0
Thiruvanthapuram	2	34	5	2	19	1	1	1	1	1	0	1	0	0	1
NDC Shastri Park	2	42	2	2	0	3	1	1	1	0	1	1	0	1	0
Gandhinagar	2	58	10	2	26	2	1	1	2	1	0	1	0	1	0
Patna	3	98	20	2	39	3	1	1	5	1	0	2	1	0	0
Raipur	2	30	14	0	14	2	1	1	0	1	0	1	0	0	1
Dehradun	2	15	10	0	15	2	1	1	0	1	0	1	0	0	1
Ranchi	2	40	14	0	14	2	1	1	0	1	0	1	0	0	1
Total	**43**	**1239**	**224**	**32**	**514**	**41**	**19**	**19**	**48**	**18**	**2**	**27**	**3**	**12**	**4**

Note1: Actual nos. of above mentioned items may vary by 5%.

Note2: The 42 U rack installed at Data Capture Centres (DCC) shall also be included in the buy back. Bidders can visit the DCC for inspection, if desired, before final bid.

Annexure – N: Qualification and Experience of Service/Resident Engineer

S.No.	Resource	Skill Set
1	2 nos. Service Engineer (RE-1) in each shift (for 24 X7) operation at each of the 3 Main Data Centres	Engineering Graduate / MCA
		One engineer certified from Proposed OEM for Compute and Storage Solution with Microsoft & Linux certification
		One engineer certified from Proposed OEM for Security (Firewall/ NIPS)
		Over 5 years of experience in respective domain
		Good communication skill
2	1 no. Resident Service Engineer (RE-2) for general shift operation at each of the 18 Data Capture Centres, and NDC, ORGI (3 shift duty only during specified period/urgency)	Engineering Graduate/ MCA / BCA with MS certification or network certification
		Over 5 years of experience in Data centre environment
		Good communication skill

ORGI

Annexure – O: STATEMENT OF DEVIATIONS FROM TECHNICAL SPECIFICATIONS

(Enclose with Technical Bid)

Line Item	Description of item specification as required by Purchaser	Description of item specification as offered by Vendor	Conformance (Yes/No)	Deviation in the offer, if any and Brief reasons for the deviation

Date:

Signature of Bidder
(Seal)

ORGI

Annexure – P: STATEMENT OF DEVIATIONS FROM TENDER TERMS AND CONDITIONS

(Enclose with Technical Bid)

Serial No:	Reference clause as per Terms and Conditions	Deviation in the offer	Brief reasons for the deviation

Date:

Signature of Bidder
(Seal)

ORGI

Annexure – Q: SCHEDULE OF DELIVERY

(Enclose with Technical Bid)

Line Item	Description of item	Quantity description	Delivery date

Date:

Signature of Bidder
(Seal)

ORGI

Annexure – R: UNDERTAKING BY THE BIDDER

(Enclose with Technical Bid)

1. **Option Clause**: The purchaser reserves the right to place order on the successful Bidder for additional quantity upto 30% of the quantity offered by them at the rates quoted at the time placement of contract or during the currency of the contract.

2. **Guarantee/Warranty**:

(i) Except as otherwise provided in the invitation to the tender the contractor hereby declare that the scanner sold/supplied to the purchaser under this contract shall be of the best quality and workmanship and new in all respects and shall strictly in accordance with the specification and particulars contained/mentioned in the contract. The contractor hereby guarantees that the said goods/stores/articles would continue to conform to the description and quality aforesaid for a period of 36 months from the date of acceptance of systems by the purchaser and the notwithstanding the fact that the Purchaser (Inspector) may have inspected and or approved the said goods/stores/articles, if during the aforesaid period of 36 months the said stores/goods/ articles be discovered not to conform to the description and quality aforesaid or not giving satisfactory performance or have deteriorated, the decision of the purchaser in that behalf shall be final and binding on the contractor and the purchaser shall be entitled to call upon the contractor to rectify the systems or such portions thereof as is found to be defective by the purchaser within a reasonable period or such specified period as may be allowed by the purchaser in his discretion on / and application made thereof by the contractor and in such an event, the above mentioned warranty period shall apply to the system rectified from the date of rectification thereof. In case of failure of the contractor to rectify or replace the goods etc. within specified time, the purchaser shall be entitled to recover the cost with all expenses from the contractor for such defective stores.

(ii) Guarantee that the product offered are not going to be declared as “End of Life (EOL)” by the OEM of concerned products, within a period of 12 months from the date of Installation in ORGI/DCOs. An undertaking from the concerned OEMs is mandatory.

ii) Guarantee that they will supply spare parts, if and when required on agreed basis for an agreed price. The agreed basis could be and including but without any limitation on agreed discount on the published catalogue or on agreed percentage of profit on the landed cost.

iii) Warranty to the effect that before going out of production for the spare parts they will give adequate notice to the purchaser of the equipment, so that the later may undertake the balance of the lifetime requirements.

iv) Warranty to the effect that they will make available the blue prints of drawing of the spares if and when required in connection with the main equipment.

3. In the event of contract being cancelled for any breach committed and the purchaser affecting re-purchase of the stores/system at the risk and the cost of the contractor, the purchaser is not bound to accept the lower offer of Benami or allied of SI-H sister concern of the contractor.

4. Purchaser will not pay separately for transit insurance and the supplier will be responsible till the entire stores contracted for, arrive in good condition at the destination. The consignee as soon as possible, but, not later than 30 days of the date of arrival of stores at destination notify of the contractor any loss or damages to the stores that may have occurred during the transit.

5. Those firms who are not specifically Registered for the items as per schedule to tender to submit the following along with their quotation failing which their offer will be ignored:-
   a. Photocopy of latest ITCC, not more than one year old.
   b. Name and full address of the banker.
   c. Prices be quoted both in words as well as in figures.
   d. Bidders who are past suppliers of the item as per T/E specification should submit their performance statement in enclosed proforma. In case, it is found that information furnished is incomplete or incorrect, their tender will be liable to be ignored.
   e. If it is intended to ask for excise duty or any other charges extra, the same must be specifically stated. In absence of such stipulation it will be presumed that prices are inclusive of all such charges and no claim for the same will be entertained.

SIGNATURE OF THE BIDDER

Date: NAME IN BLOCK LETTERS:

CAPACITY IN WHICH TENDER SIGNED

FULL ADDRESS:

Annexure-S: Format for Undertaking by the Bidder/Contractor
(To be submitted in the Stamp Paper)

Undertaking by the Bidder/Contractor

Section-I Prevention of corruption

(1) The Bidder/Contractor commits himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution:

a) The Bidder/Contractor will not, directly or through any other person or firm, offer, promise or give to EMPLOYER, or to any of EMPLOYER's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange an advantage during the tender process or the execution of the contract.

b) The Bidder/Contractor will not enter into any illegal agreement or understanding, whether formal or informal with other Bidders/Contractors. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or actions to restrict competitiveness or to introduce cartelization in the bidding process.

c) The Bidder/Contractor will not commit any criminal offence under the relevant Anti-corruption Laws of India; further, the Bidder/Contractor will not use for illegitimate purposes or for purposes of restrictive competition or personal gain, or pass on to others, any information provided by EMPLOYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d) The Bidder/Contractor of foreign origin shall disclose the name and address of the Agents/representatives in India, if any, involved directly or indirectly in the Bidding. Similarly, the Bidder/Contractor of Indian Nationality shall furnish the name and address of the foreign principals, if any, involved directly or indirectly in the Bidding.

e) The Bidder/Contractor will, when presenting his bid, disclose any and all payments he has made, or committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract and/or with the execution of the contract.

f) The Bidder/Contractor will not misrepresent facts or furnish false/forged documents/informations in order to influence the bidding process or the execution of the contract to the detriment of EMPLOYER.

g) The Bidder shall undertake that he is not supplying the similar systems or subsystems at a price lower than that offered in the present bid during the validity of period of 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 will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Buyer, if the contract has already been concluded.

h) Integrity Pact lays down the punitive actions for any violation;

(2) The Bidder/Contractor will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section-II Disqualification from tender process and exclusion from future contracts

(1) If the Bidder, before contract award, has committed a serious transgression through a violation of Section-I or in any other form such as to put his reliability or credibility as Bidder into question, EMPLOYER may disqualify the Bidder from the tender process or terminate the contract, if already signed, for such reason.

(2) If the Bidder/Contractor has committed a serious transgression through a violation of Section-I such as to put his reliability or credibility into question, EMPLOYER may after following due procedures also exclude the Bidder/Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of the transgression. The severity will be determined by the circumstances of the case, in particular the number of transgressions, the position of the transgressors within the company hierarchy of the Bidder/ Contractor and the amount of the damage. The exclusion will be imposed for a minimum of 12 months and maximum of 3 years.

(3) If the Bidder/Contractor can prove that he has restored/recouped the damage caused by him and has installed a suitable corruption prevention system, EMPLOYER may revoke the exclusion prematurely.

Section-III Liability for violation of Integrity Pact

(1) If EMPLOYER has disqualified the Bidder from the tender process prior to the award under Section-II, EMPLOYER may forfeit the Bid Guarantee under the Bid.

(2) If EMPLOYER has terminated the contract under Section-II, EMPLOYER may forfeit the Contract Performance Guarantee of this contract besides resorting to other remedies under the contract.

Section-IV Previous Transgression

(1) The Bidder shall declare in his Bid that no previous transgressions occurred in the last 3 years with any other Public Sector Undertaking or Government Department that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

_____

(For & On behalf of Bidder/Contractor)

(Office Seal)

Witness1:

Witness2:

Annexure-T: IMPORTANT DATES AND ACTIVITIES

Schedule Activities	**Date**
Earnest Money Deposit to be submitted	2,00,00,000/- (Two Crore Only)
Date of Issue/Publishing	12.09.2019
Document download start date	12.09.2019
Bid submission started	12.09.2019
Seek clarification start date	12.09.2019
Seek clarification end date	15.09.2019 till 06:50 PM
Pre-Bid Meetings	19.09.2019 (3.00 PM) at ORGI Conference hall, Wing-1, West Block-1, RK Puram, New Delhi. 07.10.2019 (4.00 PM) and 09.10.2019 (01.30PM) at ORGI Conference hall, Wing-1, West Block-1, RK Puram, New Delhi
Bid submission closing date	30.10.2019 (3:00 PM)
Date and time of opening of technical Bids	31.10.2019 (3:30 PM)
Date and time of opening of Financial Bids	After examination of technical bids by the committee.

ORGI

****** END OF RFP *******

Validate | Print | Help

m Wise BoQ

Joint Director, Office of The Registrar General, India

Name of Work: Selection of System Integrator-Hardware (SI-H) for Setting up of 3 Data Centres including installation, operation & comprehensive maintenance of Information and Communications Technology (ICT) Equipments, and Supply, installation and on-site comprehensive maintenance of Computer Hardware, related Peripheral equipments and Softwares at 18 DCCs and NDC, ORGI under Office of the Registrar General India, Ministry of Home Affairs

Contract No: 35201/02/2019-DPD (SI-H)

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

NUMBER #	TEXT #	TEXT #	NUMBER #	TEXT #	NUMBER #	NUMBER #	TEXT #
Sl. No.	Item Description	Item Code / Make	Quantity	Units	FINAL RATE (WITH GST) of items with 5 yrs comprehensive warranty/ Resident Engineer with GST In Figures To be entered by the Bidder in Rs. P	TOTAL AMOUNT (WITH GST) of items with 5 yrs comprehensive warranty/ Resident Engineer With GST in Rs. P	TOTAL AMOUNT (WITH GST) In Words
1	2	3	4	5	7	15	17
1.00	**System Integrator-hardware all kind of IT equipments/services/manpower etc to be supplied**						
1.01	Virtuliazation Software for Data Center Server	Annexure-C2	9	nos		**0.00**	INR Zero Only
1.02	Link Load Balancer	Annexure-C4	6	nos		**0.00**	INR Zero Only
1.03	Server with Enclosure Type-1	Annexure-C5(a)	21	nos		**0.00**	INR Zero Only
1.04	Server with Enclosure Type-2	Annexure-C5(b)	54	nos		**0.00**	INR Zero Only
1.05	Workstation	Annexure-C6	1,841	nos		**0.00**	INR Zero Only
1.06	Mono Laser Printer	Annexure-C7	38	nos		**0.00**	INR Zero Only
1.07	MFP Mono Printer	Annexure-C8(a)	18	nos		**0.00**	INR Zero Only
1.08	MFP Colour Printer	Annexure-C8(b)	1	nos		**0.00**	INR Zero Only
1.09	SAN Switch	Annexure-C9	8	nos		**0.00**	INR Zero Only
1.10	Core Switch Type-1	Annexure-C10	6	nos		**0.00**	INR Zero Only
1.11	Core Switch Type -2	Annexure-C11	18	nos		**0.00**	INR Zero Only

1.12	Access Switch	Annexure-C12	66	nos		**0.00**	INR Zero Only
1.13	Unified Storage (a) 1000 TB for NDC, ORGI	Annexure-C13(a)	3	nos		**0.00**	INR Zero Only
1.14	Unified Storage (b) 100 TB (Internal / External) for 5 DCC sites	Annexure-C13(b)	5	nos		**0.00**	INR Zero Only
1.15	Unified Storage (c) 75 TB (Internal / External) for 8 DCC sites	Annexure-C13(c)	8	nos		**0.00**	INR Zero Only
1.16	Unified Storage (d) 50 TB (Internal / External) for 5 DCC sites	Annexure-C13(d)	5	nos		**0.00**	INR Zero Only
1.17	Backup Software (Licences per TB) 40% of VTL Capacity	Annexure-C14	240	nos		**0.00**	INR Zero Only
1.18	Backup Appliance 200 TB	Annexure-C15(a)	3	nos		**0.00**	INR Zero Only
1.19	UPS 60 KVA	Annexure-C16	6	nos		**0.00**	INR Zero Only
1.20	UPS 80 KVA	Annexure-C17	6	nos		**0.00**	INR Zero Only
1.21	UPS 40 KVA	Annexure-C20	6	nos		**0.00**	INR Zero Only
1.22	Web Application Firewall	Annexure-C21	6	nos		**0.00**	INR Zero Only
1.23	Database Activity Monitoring (DAM)	Annexure-C22	15	nos		**0.00**	INR Zero Only
1.24	Patch Management	Annexure-C23	250	nos		**0.00**	INR Zero Only
1.25	HIPS (Servers)	Annexure-C24	100	nos		**0.00**	INR Zero Only
1.26	SIEM	Annexure-C25	1	nos		**0.00**	INR Zero Only
1.27	End Point Protection and Remediation	Annexure-C26	250	nos		**0.00**	INR Zero Only
1.28	Data Leak Prevention System (DLP)	Annexure-C27	250	nos		**0.00**	INR Zero Only
1.29	Smart Rack for 2 DR	Annexure-C28	2	nos		**0.00**	INR Zero Only
1.30	Server Rack 42 U	Annexure-C29	16	nos		**0.00**	INR Zero Only
1.31	Server Load Balancer (ADC)	Annexure-C30	6	nos		**0.00**	INR Zero Only
1.32	DDOS	Annexure-C31	6	nos		**0.00**	INR Zero Only
1.33	Network Intrusion Prevention Specifications (NIPS)	Annexure-C32	6	nos		**0.00**	INR Zero Only
1.34	Incident Response Services for SOC	Annexure-C33(a)	1	nos		**0.00**	INR Zero Only
1.35	Threat Intelligence Feed for SOC	Annexure-C33(b)	1	nos		**0.00**	INR Zero Only
1.36	On site Cyber Security Team for 60 months	Annexure-C33(c)	4	nos		**0.00**	INR Zero Only
1.37	Router for 3 DC	Annexure-C34	12	nos		**0.00**	INR Zero Only
1.38	Firewall with Virtualization	Annexure-C35	6	nos		**0.00**	INR Zero Only
1.39	Network Access Control (NAC) Authorised Hosts	Annexure-C36	250	nos		**0.00**	INR Zero Only
1.40	Anti Virus	Annexure-C37	1,966	nos		**0.00**	INR Zero Only

1.41	Situational Awareness & Analytics	Annexure-C38	3	nos		**0.00**	INR Zero Only
1.42	MS Windows server Std latest edition 16 core license bundle (for 18 Data Capture Centre)	Annexure-C1-Col5	108	nos		**0.00**	INR Zero Only
1.43	MS Windows Server Std latest edition 16 core license bundle (for 3 Datacentre)	Annexure-C2-SNo-22	105	nos		**0.00**	INR Zero Only
1.44	MS Windows CALs	Annexure-C1-Col9	1,841	nos		**0.00**	INR Zero Only
1.45	MY SQL Enterprise Server (Latest Edition) for 18 Data Capture Centres & 3 DCs.	Annexure-C3-Col4	22	nos		**0.00**	INR Zero Only
1.46	MS Office Professional 5 users server based Latest Version 18DCC an 3 DCs	Annexure-C3-Col3	41	nos		**0.00**	INR Zero Only
1.47	Visual Studio Latest Enterprise Version	Annexure-C2-SNo-23	1	nos		**0.00**	INR Zero Only
1.48	Per month Salary of Resident Engineer for NDC & 2 DR sites (3 Shifts) (RE-1) for first 24 months	No Annexure-1	24	nos		**0.00**	INR Zero Only
1.49	Per month Salary of Resident Engineer for NDC & 2 DR sites (General Shift) (RE-1) for 36 months, After 24 months mentioned in Item 48(a)	No Annexure-2	12	nos		**0.00**	INR Zero Only
1.50	Per month Salary of Resident Engineer for DCCs (RE-2) for 60 months	No Annexure-3	19	nos		**0.00**	INR Zero Only
1.51	**Buy Back of old equipments From 18 Location as per annexure M**	**Buy Back of Hardware items**	**1**	nos		**0.00**	INR Zero Only
Total in Figures						**0.00**	INR Zero Only
Quoted Rate in Words					**INR Zero Only**		

1	System Integrator-hardware all kind of IT e			Constructi	item1	10	1 Nos
1.01	Virtuliazati	Annexure-	9	nos	Supplying	item1	123.223 Nos
1.02	Link Load	Annexure-	6	nos	Supplying	item1	123.223 Nos
1.03	Server wit	Annexure-	21	nos	Supplying	item1	123.223 Nos
1.04	Server wit	Annexure-	54	nos	Constructi	item2	213 Nos
1.05	Workstatic	Annexure-	1841	nos	Constructi	item3	10 Nos
1.06	Mono Las	Annexure-	38	nos	Supplying	item1	123.223 Nos
1.07	MFP Mon	Annexure-	18	nos	Constructi	item2	213 Nos
1.08	MFP Colo	Annexure-	1	nos	Constructi	item3	10 Nos
1.09	SAN Swit	Annexure-	8	nos	Supplying	item1	123.223 Nos
1.1	Core Swit	Annexure-	6	nos	Constructi	item2	213 Nos
1.11	Core Swit	Annexure-	18	nos	Constructi	item3	10 Nos

1.12	Access Sv	Annexure-	66	nos	Supplying	item1	123.223	Nos
1.13	Unified St	Annexure-	3	nos	Constructi	item2	213	Nos
1.14	Unified St	Annexure-	5	nos	Constructi	item3	10	Nos
1.15	Unified St	Annexure-	8	nos	Supplying	item1	123.223	Nos
1.16	Unified St	Annexure-	5	nos				
1.17	Backup S	Annexure-	240	nos	Constructi	item2	213	Nos
1.18	Backup Ap	Annexure-	3	nos	Constructi	item3	10	Nos
1.19	UPS 60 K'	Annexure-	6	nos	Constructi	item3	10	Nos
1.2	UPS 80 K'	Annexure-	6	nos	Supplying	item1	123.223	Nos
1.21	UPS 40 K'	Annexure-	6	nos	Supplying	item1	123.223	Nos
1.22	Web Appli	Annexure-	6	nos	Constructi	item2	213	Nos
1.23	Database	Annexure-	15	nos	Constructi	item3	10	Nos
1.24	Patch Mar	Annexure-	250	nos	Supplying	item1	123.223	Nos
1.25	HIPS (Ser	Annexure-	100	nos	Constructi	item2	213	Nos
1.26	SIEM	Annexure-	1	nos	Constructi	item3	10	Nos
1.27	End Point	Annexure-	250	nos	Supplying	item1	123.223	Nos
1.28	Data Leak	Annexure-	250	nos	Constructi	item2	213	Nos
1.29	Smart Rac	Annexure-	2	nos	Constructi	item3	10	Nos
1.3	Server Ra	Annexure-	16	nos	Supplying	item1	123.223	Nos
1.31	Server Lo	Annexure-	6	nos	Constructi	item2	213	Nos
1.32	DDOS	Annexure-	6	nos	Constructi	item3	10	Nos
1.33	Network Ir	Annexure-	6	nos	Supplying	item1	123.223	Nos
1.34	Incident R	Annexure-	1	nos	Constructi	item2	213	Nos
1.35	Threat Int	Annexure-	1	nos	Constructi	item3	10	Nos
1.36	On site Cy	Annexure-	4	nos	Supplying	item1	123.223	Nos
1.37	Router for	Annexure-	12	nos	Constructi	item2	213	Nos
1.38	Firewall w	Annexure-	6	nos	Constructi	item3	10	Nos
1.39	Network A	Annexure-	250	nos	Supplying	item1	123.223	Nos
1.4	Anti Virus	Annexure-	1966	nos	Constructi	item2	213	Nos

1.41	Situationa	Annexure-	3	nos	Constructi	item3	10	Nos
1.42	MS Windc	Annexure-	108	nos	Supplying	item1	123.223	Nos
1.43	MS Windc	Annexure-	105	nos	Constructi	item2	213	Nos
1.44	MS Windc	Annexure-	1841	nos	Constructi	item3	10	Nos
1.45	MY SQL E	Annexure-	22	nos	Supplying	item1	123.223	Nos
1.46	MS Office	Annexure-	41	nos	Constructi	item2	213	Nos
1.47	Visual Stu	Annexure-	1	nos	Constructi	item3	10	Nos
1.48	Per month	No Annex	24	nos	Constructi	item3	10	Nos
1.49	Per month	No Annex	12	nos	Supplying	item1	123.223	Nos
1.5	Per month	No Annex	19	nos	Constructi	item2	213	Nos
1.51	Buy Back	Buy Back	1	nos	Constructi	item3	10	Nos
					4 Constructi	item5	10	Nos