रेलटेलकॉर्पोरेशनऑफइंडियालिमिटेड
(भारतसरकारकाएकउपक्रम)

RAILTEL CORPORATION OF INDIA LIMITED
(A Govt. of India Undertaking)

ELECTRONIC TENDER DOCUMENT

FOR

"रेलटेल के डाटा सेंटर (डीसी एंड डीआर) के लिए सुरक्षा समाधान और क्लाउड इन्फ्रास्ट्रक्चर का विस्तार हेतु आपूर्ति, स्थापना, परीक्षण और कमीशन"

Supply, Installation, Testing &Commissioning of Security Solution and Expansion of Cloud Infrastructure for Data Center (DC & DR) of RailTel.

(Through e-Reverse Auction)

E-निविदासंख्या: RAILTEL/TENDER/OT/CO/DNM/2019-20/DC Security & Cloud Infra/489

OPEN E-TENDER NO.RAILTEL/TENDER/OT/CO/DNM/2019-20/DC Security & Cloud Infra/489

निविदादस्तावेजकीकीमत: रु.11,800/-(टैक्ससहित)
Cost of Tender Document: Rs. 11,800/- (Including Taxes)

Sold to _____

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area, Sector -44
Gurgaon-122003, Ph: 0124-4236085-86, Fax: 0124-4236084

E-Tender Notice No.: RAILTEL/TENDER/OT/CO/DNM/2019-20/Security & Infra Solution of DC & DR /489 Dtd. 06.06.2019

RailTel Corporation of India Ltd. (RailTel) invites E-Tenders through reverse auction in Two Packet (Part I –Credential/ Techno commercial Bid and Part II - Price Bid) System for **"Supply, Installation, Testing & Commissioning of Security Solution and Expansion of Cloud Infrastructure for Data Center (DC & DR) of RailTel"**.

a)	Opening date of Tender downloading	07.06.2019
b)	Submission date of bids	28.06.2019 up-to 15:00 hrs.(Online)
c)	Opening of bids	28.06.2019 at 15:30 hrs (Online)
d)	Approximate cost of Tender	Rs 21.48 Croreapprox (Inclusive All.)
e)	Earnest Money (EMD) #	Rs 12,24,000/- to be made infavor of RailTel Corporation of India Ltd.in the form of DD payable at New Delhi.
f)	Cost of Tender Document is Rs.11,800/-(Including Tax)	

Small scale Units registered with NSIC and MSME under single point registration scheme are exempted from cost of Tender Documents and EMD.

Note: Tender Notice and Tender Document are available on RailTel's website and can be downloaded from **www.railtelindia.com** or from the e-Tendering portal https://www.ireps.gov.in. For online bid submission the bidder will have to necessarily download an official online copy of the tender documents from IREPS e-portal. All future Information viz. corrigendum /addendum/ amendments etc. for this Tender shall be posted on the e-Tendering Portal only. Printed copy of Tender document will not be sold from RailTel office.

The bidder shall bear all costs associated with the preparation, submission/participation in the bid. Purchaser in no way will be responsible or liable for these costs regardless of the conduct or outcome of the bidding process.

INDEX

CHAPTER-1

OFFER LETTER

RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

1. I/We _____ have read the various conditions detailed in tender documents attached here to and hereby agree to ABIDE BY THE SAID CONDITIONS. I/We also agree to keep this offer open for acceptance for a period of 60 days from the date of submission and in default thereof. I/We will be liable for forfeiture of my/our Earnest Money. I/We offer to supply various equipment at the rates quoted in the attached schedules and hereby bind myself/ourselves to complete the work of**"Tender document for Supply, Installation, Testing & Commissioning of Security Solution and Expansion of Infrastructure for Data Center (DC & DR) of RailTel"**within 120days from the date of issue of Purchase Order. I/We also hereby agree to abide by the Various Conditions of Contract and to carry out the supplies according to the Specifications for materials and works laid down by the RailTel.

2. Earnest Money of Rs……. has been submitted through IREPS portal with the following transaction details:

The full value of Earnest Money shall stand forfeited without prejudice to any other rights or remedies if, I/We withdraw or modify the offer within validity period or do not deposit the security deposit (Performance Bank Guarantee) within specified days as per tender after issue of Purchase Order/LOA.

SIGNATURE OF SUPPLIER (S)

Date:

CONTRACTOR (S) ADDRESS

SIGNATURE OF WITNESS:

1.

2.

CHAPTER- 2

SCHEDULE OF REQUIREMENT

SOR	ITEM DESCRIPTION	UOM	QTY	Unit Rate (All inclusive) (in Rs.)		Total Cost (in Rs.)	
				In Fig	In word	In Fig	In word
SOR-A	Web Application Firewall as per Technical Specification given in Chapter-3A	Nos	04				
SOR-B	Backup Solution as per Technical Specification given in Chapter-3A	Nos.	01				
SOR-C	UTM &Virtual Firewallas per Technical Specification given in Chapter-3A						
i)	Virtual Firewall Instance –L3	Nos.	03				
ii)	UTM	Nos.	02				
iii)	Firewall Manager (For virtual Firewall instances +UTM)	No.	01				
SOR-D	Security Detection and Analyticas per Technical Specification given in Chapter-3A						
i)	Commercial SOC includes software components SIEM Inncident forensic and packet capture.	Nos.	01				
ii)	Anti-Virus +EDR (Client)	Lot	01				
iii)	Anti-Virus + EDR (Server)	Lot	01				
iv)	Vulnerability Assessment Software Solution	Nos,	01				
SOR-E	Cloud Solution in RailTel Data Center as per Technical Specification given in Chapter-3A						
i)	Rack Server	Nos	24				
ii)	10G Switch as	Nos	04				
iii)	Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License	lot	01				
SOR-F	One time charges for installation & commissioning of whole system and integration with existing system.	Nos	01				
Sub Total							
SOR-G	Incremental% AMC cost in addition to 3.5 % mentioned in clause 3 of Chapter-4	Years	05				
Grand Total							
Grand Total (In Words)							

Note:	
I.	a)Unit rate quoted against SOR above should be CIP destination inclusive of all duties, taxes, insurance and freight etc (with tax break-up as per Performa attached as Annexure-A).The materials as per SOR are required to be delivered within the delivery period as indicated in Bid Data Sheet(BDS, Chapter 5) to the site /transported to different locations which will be provided by RailTel to the successful bidder. b)It shall be the responsibility of Tenderer to transport the equipment to site for Installation & Commissioning.
II.	Tenderers should submit the detailed configuration of each type of equipment indicating quantities of various modules/sub modules/cards/Licenses/sub racks including the vacant slots in the sub racks/chassis for further expansion. Detail BOM of each equipment supplied under the contract shall be submitted along with the bid and the same shall be duly vetted by the OEM.
III.	The Tenderer shall attach Unit Rate Analysis of Schedule of Requirements (cost of each sub-assembly, card, module, Licenses etc.) in their Price Bid. The quoted Unit Ratesshould correspond to the referred unit Rate.
IV.	Tenderer must also furnish unit rate of all the supply of items mentioned in the SOR, which will be required for the Solution. These will also form part of the Rate Contract for procurement of items as when required.
V.	The tenderer will be fully responsible Supply ofEquipment/cards/interfaces and all related items for installation and commissioning ofthe network including the following: a) Integration with existing Network as required. b) Spares required for Commissioning, maintenance supervision & warranty period shall be maintained by the Contractor at his own cost. c) All necessary cables and connectors and other accessories required for installation.
VI.	Tenderer should be an Original Equipment Manufacturer (OEM) or Authorized representative of OEM
VII.	The Bidder should have authorization specific to this tender from respective OEM. Bidder has to quote only one OEM against one SOR
VIII.	Bidder has to quote for all SOR and evaluation will be done on totality.

****

Annexure-A
Tax Breakup for SOR

SOR	Description	Total Qty	Basic Unit Price (exclusive of all levies and charges)	Pkg & Forwarding Charges		Freight & Insurance Charges		CGST/SGST/ IGST/UTGST etc.		Price Per Unit (all inclusive) for delivery at destination (In Rs.) (4+6+8+10)	
				%	Amt	%	Amt	%	Amt	In Fig	In Word
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
SOR-A											
SOR-B											
SOR-C-i											
SOR-C-ii											
SOR-C-iii											
SOR-D-i											
SOR-D-ii											
SOR-D-iii											
SOR-D-iv											
SOR-E-i											
SOR-E-ii											
SOR-E-iii											
SOR-F											

Note: The rate quoted at IREPS Portal will be final. Bidder may submit the price breakup as per format given above.

Chapter - 2-A

These are the Special Instructions to the Bidders for e-Tendering.

Submission of Bids only through online process is mandatory for this Tender

E-Tendering is a new methodology for conducting Public Procurement in a transparent and secured manner. Now, the Government of India has made e-tendering mandatory. Suppliers/ Vendors will be the biggest beneficiaries of this new system of procurement. For conducting electronic tendering, RailTel has decided to use the portalhttps://www.ireps.gov.in, Indian Railways E-Procurement system (IREPS).

Benefits to Suppliers are outlined on the Home-page of the portal. Bidders are advised to visit the IREPS Portal for details related to E-Tender i.e. Registration, FAQ, Helpdesk, Learning Center etc.

1. **Tender Bidding Methodology:**

   Sealed Bid System - 'Single Stage - Two Envelope': In this, bidder has to submit each the bid (Part I –Credential/ Techno commercial Bid and Part II - Price Bid) in separate envelope "ONLINE".

   IREPS Helpdesk

   Please visit Helpdesk section on IREPS Portal.

   ### RailTel Contact-I (for general Information)

   RailTel's Contact Person /Designation
   Rajeev Kumar, Sr. Manager/DNM
   Telephone/ Mobile: 9717644419
   E-mail ID: rajeevkumar@railtelindia.com

   ### RailTel Contact-II (for general Information)

   RailTel's Contact Officer
   A. K. Sablania, ED/DNM
   Telephone/ Mobile: 9717644015
   E-mail ID: asablania@railtelindia.com

2. **Bid related Information for this Tender (Sealed Bid)**

   The entire bid-submission would be online on IREPS Portal.

   Broad outline of submissions are as follows:

   a. Submission of Bid Security/ Earnest Money Deposit (EMD)
   b. Submission of digitally signed copy of Tender Documents/Addenda
   c. Two Packet (Part I –Credential/ Techno commercial Bid and Part II - Price Bid)

d. Online response to Terms & Conditions of Tender.
e. (Optional) Online Submission of modification, substitution bids for technical or financial parts, or withdrawal bid.

NOTE: Bidder must ensure that the bid must be successfully submitted online as per instructions of IREPS Portal.

3. Offline Submissions:

The bidder is required to submit the following documents offline to RailTel Corporation of India Ltd, Institutional Area, Plot 143, Sector 44, Gurgaon, before due date & time of submission of bids specified in this tender document, in a Sealed Envelope. The envelope shall bear (the tender name), the tender number and the words 'DO NOT OPEN BEFORE' (due date & time).

a. Power of attorney to be submitted in accordance with Clause-34.5, Chapter-4 of Tender Document.

b. Specific authorization addressed to RailTel from the OEM (Parent Company) for Indian Subsidiary (Clause 4.A.14 of Tender Document).

c. System Performance Guarantee (Form no. 2, Chapter-6) on stamp paper of Rs. 100/-.

d. Duly filled & signed Integrity Pact Proforma on Rs 100/- stamp paper (2 copies) (for the tender value exceeding Rs. 15 crores at a time) and to be uploaded on IREPS website also (Form No. 5 of Chapter-6).

Format for Affidavit as per Form-4 failing which BID WILL BE SUMMARILY REJECTED.

NOTE: The Bidder has to upload the Scanned copy of all above original documents as Bid-Annexures during Online Bid-Submission.

(Nomenclature of uploaded file should be proper and as per submitted documents)

4. Submission of Eligibility Criteria related documents:

Eligibility criteria related documents as applicable shall also be scanned and submitted ONLINE.

NOTE:In case of internet related problem at a bidder's end, especially during 'critical events' such as - a short period before bid-submission deadline, during online public tender opening event, during e-auction, it is the bidder's responsibility to have backup internet connections.

In case there is a problem at the e-procurement/ e-auction service provider's end (in the server, leased line, etc) due to which all the bidders face a problem during critical events, and this is brought to the notice of RailTel by the bidders in time, then RailTel will promptly re-schedule the affected event(s).

5. Instructions for Tender Document TO THE BIDDERS

The RailTel Tenders are published on www.railtelindia.com and on IREPS Portalhttps://www.ireps.gov.in/.

NOTE: For online bid submission the bidder will have to necessarily download an official online copy of the tender documents from IREPS portal, and this should be done well before the deadline for bid-submission.

6. Submission of Offers and Filling of Tender:

This e-tender should be duly submitted online using the e-Procurement Portal https://www.ireps.gov.in/.For detailed instructions please refer to IREPS Portal.

7. Fax Quotations & Late Tenders:

Fax Tender documents and Late/Delayed tenders would not be considered.

8. Attendance of Representatives for Tender Opening:

Representatives of bidders desirous to attend the tender opening can do so on production of a proper letter of authority from the respective firm, failing which they may not be allowed to attend the tender opening. Authorized representatives of those firms who have submitted the tender documents alone shall be allowed to attend the tender opening.

9. Addenda / Corrigenda:

Addenda / Corrigenda to the tender documents may be issued by RailTel prior to the date of opening of the tenders, to clarify or reflect modifications in the contract terms and conditions or in the design. Such addendum/corrigendum shall be available on IREPS and RailTel Portal only. Bidders who are unable or unwilling to bring their tenders to conform to the requirements of the RailTel are liable to be rejected.

10. Ambiguity/ Pre- Bid Clarification Requests:

If there is any ambiguity or doubt as to the meaning of any of the tender clauses/ conditions or if any additional information required, the matter should immediately be referred to the RailTel in writing through emails to RailTel Contacts defined above.

11. Bid submission and Opening date

a. The bid should be submitted online along with Credential/Techno commercial & Price bid document (all documents).

b. The bidder's bids will be opened at the time & date of opening of the tender given in the Bid Data Sheet (BDS) online simultaneous in presence of such Bidders/ Representatives who choose to be present online. The Tenders/Representatives can also choose to be physically present in the office of RailTel for the Online Public Tender Opening Event.

c. Bidder need to be submitted offline document listed above before due date and time of tender opening.

12. e-Reverse Auction: The procurement in this tender will be done on reverse auction.

a. In addition to the instructions given in above, the bids shall be processed through Two Stage Reverse Auction method, to be implemented through IREPS portal. Two packets system shall be followed for the 1st stage of reverse auction, which means that Techno-commercial bid will be opened first; and after deciding the suitability or otherwise of the technical bids, the financial bids of only those firms which are found to be suitable shall be opened.
(For details please refer also user manual for contractors-for Two Stage Reverse Auction (Goods & Services Module) of IREPS available on IREPS portal.)

b. The financial bid of those firms whose technical bids have been found to be suitable shall be opened on or after scheduled date and time. The financial tabulation statement shall be generated immediately thereafter, and can be viewed by the participating bidders by logging into IREPS account.

c. After opening the financial bids, the tendering department shall schedule the start of reverse auction. The tenderers who are eligible for the participation in the reverse auction process can view the reverse auction catalogue by logging into their IREPS account.

d. The lowest Initial Price Offer (L1 offer price) as submitted by the technically qualified bidders during the financial evaluation stage shall constitute the base price for starting the reverse auction. The base price shall be notified to the bidder.

e. Date and time of start of RA will be informed by IREPS website/RailTel Website.

f. Selection of vendors for RA shall be as under:
If the number of tenderers qualified for award of contract is less than 3, No RA shall be conducted and the tender shall be decided on the basis of initial price offer.

If the number of tenderers qualified are 3 to 6, only 3 tenderers shall be eligible for participating in RA.

If the number of tenderers qualified are more than 6, only 50% of tenderers shall be eligible for RA (rounded off to next higher integer).

The bids disallowed from participating in the RA shall be the highest bidder(s). In case the highest bidders quote the same rate, the initial price offer received last as per time log of IREPS, shall be removed first, on the principle of last in first out, by IREPS system itself.

Initial Cooling Off period shall be 2 hours.

Auto Extension Period shall be 10 minutes.

Minimum Decrement in percentage shall be 0.1% of Current Lowest Bid.

g. Once the reverse auction process is closed the lowest rate received in the reverse auction/financial offer will be evaluated. RailTel reserved the right not to consider the lowest bid received in the reverse auction/financial bid process.

h. In case of no participation in RA process by any bidder, the base value of RA process will be considered for commercial bid assessment.

i. Technical e-RA training can be opted by the bidder to know the procedure of e-RA (Reverse Auction).

j. RailTel may discharge the tender at any stage without assigning any reason.

k. Bidders may please note that Bidding close Date/Time gets extended automatically every time an offer is received against the tender during a time interval equivalent to Cooling Off prior to the closing date and time. For example: If the Closing Time of RA is 13:00 Hrs and the Cooling Off period is 20 Minutes, if two offers are received between 12:30 Hrs and 13:00 Hrs, lets say at 12:40 Hrs and 12:55 Hrs, the Closing Time shall be extended by 30 Minutes from the time of submission of the last bid i.e. up to 13:25 Hrs.

13. Award of Contracts, Financial Evaluation & Reverse Auction (e-RA):

After the evaluation of technical proposals, the financial bids (initial price offer) of those firms whose technical bids meet eligibility criteria shall be categorized as qualified for the purpose of Reverse Auction (e-RA). These financial bids shall be opened on the scheduled date and time (as per procedure explained in the IREPS User Manual for vendors – Two Stage Reverse Auction Goods & Services Module para C, D and E available at IREPS Helpdesk & Learning Centre). The e-RA procedure has been implemented through IREPS Portal and as per guidelines issued by Ministry of Railways Letter No. 2017/Trans/01/Policy/Pt-S Dated 28.03.2018. As per the procedure a minimum of three bids are mandatory for conduct of e-RA. In case the numbers of qualified bids are less than three, the L-1 would be decided on the initial price offer quoted by the bidder by IREPS. In case of more than three qualified bidders, the e-RA as explained in the manual mentioned above will be implemented. After the end of e-RA, L-1, L-2 and so on identified.

CHAPTER-3-A

Technical Requirement

The bidder has to carry out following activities: -

1. Supply, Installation, Configuration, performance Tuning & Integration, Performance Testing, Acceptance Testing, Commissioning and Training of the supplied hardware, software, network equipment and network & security software as per Schedule of Requirements.

2. Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM professional services for the supplied Hardware, Software, Network equipment and Network & Security software for their installation, configuration, fine-tuning, integration with existing components and commissioning to meet the functional requirements. OEMs shall also be responsible for successful implementation and system operations.

3. Comprehensive Warranty support services of all supplied Hardware, Network equipment and Cabling for all the supplied Software and Network & Security software valid for a period of 36 months from the Date of System Commissioning or 40 months from the date of delivery to the site (Only in case the delay in system commissioning is on the part of consignee), whichever is earlier.

Note 1: It may kindly be noted that in the specification wherever support for a feature has been asked for, it will mean that the feature should be available without RailTel requiring any other hardware/software/licenses. Thus, all hardware/software/licenses required for enabling the support/feature shall be included in the offer.

Note 2: Bidder should submit the vetted BOM from their respective OEMs.

Note 3:The Bidder should have OEM authorization specific for this tender.

Note 4: Bidder has to provide all type of optics (SFP/ SFP+/XFP/QSFP28 etc.) of same OEM offered against SOR and Passive component (Patch Cords & other items) required for Installation and Commissioning of complete solution should be from reputed OEM.

SOR-A:Web Application Firewall:

SN	Minimum Requirement Description
1	The solution's monitoring appliance must be able to support ALL of the following deployment modes to monitor web application traffic over the network: - Via a SPAN/TAP port sniffing mode - Layer-2 transparent inline mode - Reverse Proxy mode - Transparent Layer-2 Reverse Proxy mode

2	The solution must support the following authentication mechanism for accessing the solution management UI: - In-built authentication in the solution - Kerberos authentication - LDAPS authentication and authorization with the following Windows platforms: 2003, 2003 R2, 2008, 2008 R2, 2012, and 2012 R2. - RADIUS authentication
3	The solution must support the following password management capabilities without relying on any external system: a) Password validity period in days b. Password length (minimum required number of characters in the password.) c. Whether a password must be significantly different from the last password used d. Whether a password must include capital letters, numbers, lower case letters and non alpha-numeric characters or not.
4	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management
5	The solution should prevent the following attacks (but not limited to): a) Brute force /DDOS b) Access to predictable resource locations c) Unauthorized navigation d) Web server reconnaissance e) HTTP request format and limitation violations (size, unknown method, etc.) f) Use of revoked or expired client certificate g) File upload violations.
6	The solution must provide the following features and protection: - HTTP protocol validation - Correlated based attack protection - HTTP protocol attack signatures - Cookie signing validation - Anti site scraping - Bot mitigation - Whitelisting based protection - Web worm protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation - Proactive bot Defense with ability to detect if the Bots are using Captcha farms to bypass the Captcha challenge. - Sensitive data exposure - Behavioral & Stress based detection - Heavy URL protection - Sloris attacks - Web Page parameter Security - forcefull Browising - Cookie Tampering
7	The solution must support the positive security model approach. A positive security model states what input and behaviour is allowed and everything else that deviates from the positive security model is alerted and/or blocked.

8	The solution must support the negative security model approach. A negative security model explicitly defines known attack signatures.
9	The solution must be able to block transactions with content matching known attack signatures while alllowing everything else.
10	The solution must be able to support both inline and non-inline monitoring-only and active enforcement mode. In monitoring-only mode, the administrator can view alerts, attacks, server errors, and other unauthorized activity. In active enforcement mode, the solution can perform everything that is done in monitoring-only mode and additionally be able to block attacks.
11	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: - Ability to drop requests and responses, - Block the TCP session, - Block the application user, or - Block the IP address
12	WAF support the following normalization methods:
	a) URL-decoding (e.g. %XX)
	b) Null byte string termination
	c) Self-referencing paths (i.e. use of /. / and encoded equivalents)
	d) Path back-references (i.e. use of /.../ and encoded equivalents)
	e) Mixed case
	f) Excessive use of whitespace
	g) Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)
	h) Conversion of (Windows-supported) backslash characters into forward slash characters.
	i) Conversion of IIS-specific Unicode encoding (%uXXYY)
	j) Decode HTML entities (e.g. c, ", ª)
	k) Escaped characters (e.g. \t, \001, \xAA, \uAABB).
13	The solution must be able to block the user or the IP address for a configurable period of time.
14	The solution must be able to send a TCP RST packet to both ends of a web connection when it is deployed in sniffing mode in the event of active enforcement deployment mode.
15	The solution must be able to protect both HTTP Web applications and SSL (HTTPS) web applications.
16	The solution must be able to decrypt SSL web traffic between clients and web servers.
17	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the monitoring appliance deployed in transparent layer-2 mode.
18	The solution must provide the ability to comply to A+ Certification at the click of a button
19	The solution must provide the ability to control SSL settings via a GUI based interface.
20	The solution must be able to decrypt SSL web traffic for inspection without terminating or changing the HTTPS connection.
21	The solution must include a pre-configured list of comprehensive and accurate web attack signatures.
22	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.

23	The solution must provide signature protection against known vulnerabilities in commercial infrastructure software such as Apache, IIS and so on. The content provided by the signature detection mechanism must be based on the research done by the solution vendor threat intelligence division and a combination of other resources such as Snort, CVE and so on. This set of signatures must be continuously and automatically updated.
24	The solution must allow administrators to add and modify signatures.
25	The solution must support regular expressions for the following purposes: - Signatures definition - Sensitive data definition - Parameter type definition - Host names and URL prefixes definition - Fine tuning of parameters that are dynamically learnt from the web application profile
26	The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats.
27	The solution must be able to detect known attacks at multiple levels. This includes network, Web server software and application-level attacks.
28	The solution's in-built corrleation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic.
29	The solution must inspect and monitor all HTTP(S) data and the application level including HTTP(S) headers, form fields, and the HTTP(S) body.
30	The solution must be able to inspect HTTP requests and responses.
31	The solution must be able to identify WebSocket connections.
32	The solution must be able to validate encoded data in the HTTP traffic.
33	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.
34	The solution must be capable of automatically create whitelisting/profiling of web applications.
35	The solution profiling technology must be able to detect and protect against threats which are specific to the custom code of the web application. After the profiling/learning phase, the solution must be able to understand the structure of each protected URL.
36	The solution must automatically build/learn the web application profiles and use them to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.
37	The solution must be able to automatically learn the web usage and application structure and elements and expected user behaviors as soon as the system is installed. The structure and elements include URLs, directories, cookies, form fields and parameters, and HTTP methods. User behaviors include expected value length; acceptable characters per parameter field; whether the parameter value is read-only or editable by the user and whether the parameter is mandatory or optional.
38	The solution profiling learning mode must be able to recognize changes to the web application and simultaneously protect web applications at the same time.
39	The solution must be able to learn and create profile and in parallel should protect application by blocking malicious requests using negative security model based policies.
40	The solution must allow profiles to be manually changed and information can be added and removed to fine tune the profiles.

41	The solution must support profiling from only a set of trusted users to learn the normal acceptable behavior and usage of the web application.
42	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.
43	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in learning mode.
44	The solution must be able to perform profiling of web applications in an environment where there is a mixture of good and bad traffic. The solution must be able to automatically differentiate good and bad traffic when learning the profile. Bad traffic should not be learnt.
45	The solution must be able to automatically learn all the host names of the web applications being protected.
46	The solution must be able to perform profiling of JSON. HTTP requests in the JSON format must be learnt by the WAF with the paramters and values.
47	Web application firewall should support stress based application DDOS detection and should be capable of building real time L7 signatures based on machine learning and behavioral analysis.
48	The solution must be able to protect web applications that include Web services (XML) content.
49	The XML protection offered by the solution must be similar to the web application protection provided with automated profiling/learning capability.
50	The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria. This should be possible without need to write any script/code.
51	The solution must be able to digitally sign cookies, encrypt cookies, and to rewrite URLs when it is deployed in the reverse proxy mode.
52	The solution must support both URL rewriting and content rewriting for http header and body when it is deployed in the reverse proxy mode.
53	The solution must be able to perform virtual patching for its protected web applications.
54	The solution must be able to track and monitor web application users. This user tracking mechanism must be automated, with no changes to the existing application or authentication scheme.
55	The solution must support user tracking using both form-based and certificate-based user authentication.
56	Should meet all applicable PCI DSS requirements pertaining to system components in the cardholder data environment, should also monitor traffic carrying personal information.
57	Should have the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.
58	Should inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)
59	WAF should support dynamic source IP blocking and should be able to block attacks based on IP source.
60	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.

61	Inspect any web socket protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data are not otherwise inspected at another point in the message flow.
62	WAF should support inline bridge or proxy mode of deployment.
63	WAF should have an option to configure in Reverse proxy mode as well.
64	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.
65	Transactions with content matching known attack signatures and heuristics based should be blocked.
66	The WAF database should include a preconfigured comprehensive and accurate list of attack signatures.
67	The Web application firewall should allow signatures to be modified or added by the administrator.
68	The Web application firewall should support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.
69	WAF should support different policies for different application sections.
70	The Web application firewall should automatically learn the Web application structure and elements.
71	The Web application firewall learning mode should be able to recognize application changes as and when they are conducted.
72	The WAF should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc.
73	The Web application firewall should support line speed throughput and sub-millisecond latency so as not to impact Web application performance.
74	For SSL-enabled Web applications, the certificates and private/public key pairs for the Web servers being protected need to be up loadable to the Web application firewall.
75	The Web Application Firewall should have "anti-automation" protection which can block the automated attacks that use hacking tools, scripts, frame work etc.
76	The Web application firewall should have an out-of band management port.
77	The Web application firewall should support web based or a centralized management and reporting for multiple appliances.
78	Bidder should be able to deploy the Web application firewall and remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.
79	The Web application firewall should be able to generate custom or pre-defined graphical reports on demand or scheduled.
80	The Web application firewall should provide a high level dashboard of system status and Web activity.
81	Should be able to generate comprehensive event reports with filters:
	a. Date or time ranges
	b. IP address ranges
	c. Types of incidents
	d. Geo Location of attack source
	d. Other (please specify).
82	The following report formats are deemed of relevance: Word, RTF, HTML, PDF, XML, etc.

83	The appliance based solution should support Inline, Reverse Proxy mode of deployment.
84	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair), and included with every log message.
85	Web application firewall should provide notifications through Email, Syslog, SNMP Trap etc.
86	WAF should be able to log full session data once a suspicious transaction is detected.
87	Should be simple to relax automatically-built policies.
88	The solution should provide the admin to manually accept false positives.
89	Should be able to recognize trusted hosts.
90	The WAF in passive mode should be able to provide impact of rule changes as if they were actively enforced.
91	Should support clustered deployment of multiple WAFs sharing the same policy.
92	The solution should support virtual environments.
93	The solution should have the capability of load balancing between the applications in an active – active environment.
94	The Web application Firewall should support authentication with LDAP and radius server.
95	The Solution should allow commands like PING, trace route, telnet from WAF for troubleshooting network related issues.
96	The Solution should have option to configure NTP server details.
97	Support should include 3 years onsite Premium OEM warranty 24 x 7 support with Next business Day (NBD) Shipment
98	The solution should have network routing feature.
99	In case of RMA Process, Define the no of days to deliver the solution.
100	Should support both IPv4 and IPv6
101	The solution must support the web application vulnerability assessment tools (Web application scanners in Leaders of Latest Gartner Magic Quadrant Application Security Testing) to virtually patch web application vulnerabilities. Like:- - Acunetix - Beyond Security - Cenzic - Denim Group - HP Fortify WebInspect - IBM AppScan - NT OBJECTives - Qualys - Rapid7 - Trend Micro - Veracode - WhiteHat
102	The solution must be able to support 2 Gbps of WAF (HTTPS) throughput
103	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019
104	System must have minimum(fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.
105	The proposed appliance should support Hardware based HTTP Compression, that is 20Gbps of Hardware compression from day one
106	The proposed appliance should support 20Gbps of Bulk Encryption from day one

107	The proposed Appliance should be with perpetual WAF license
108	the proposed solution should have 64bit OS architecture
109	the proposed appliance should have capability of Hardware based DDOS protection up to 50M Sync Cookies per second
110	The proposed hardware should include a LCD panel which should support Configuration for Initial Management IP address and display all the error and information corresponding to hardware & software without logging into the appliance.
111	The proposed appliance should be of 1U/2U form-factor
112	The proposed appliance should have minimum of 45GB of RAM on day 1
113	the proposed appliance should have minimum of 450GB of SSD Hard Drive for better performance from day one
114	The Solution shall support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 draft
115	The proposed appliance should support up to 35K SSL TPS with Dedicated SSL Offloading Chip. TPS = Only one HTTP transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.
116	The offered system must support Hardware offload using dedicated SSL Card for Perfect Forward Secrecy (PFS) with Elliptic Curve DiffieHellman Exchange (ECDHE) and other Elliptic Curve Cryptography (ECC) ciphers.
117	The solution should have dual power supply fully populated (within box) from day one and should support AC Power Supply
118	OEM Should have a development center in India for a better support
119	The solution should support all operating systems and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris, HP Unix.
120	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair), and included with every log message.
121	Should be able to encrypt the user credentials in real time so as to protect any sensitive parameter as defined by department to protect from keyloggers and credential stealing malware residing in the end users system
122	WAF should protect against L7 Latency Based denial of service Attacks and should support detection of attacks based on transaction rates on the client side (TPS-based) and latency on the server side (stress-based)
123	Should support client certificate constrained delegation (C3D) which will enable the Load balancing solution to generate certificates on behalf of clients and pass it to the end servers if SSL based client authentication has been enabled on the backend servers .
124	Should Support Active/Standby, Active/Active & N+1
125	Should Support Session Mirroring Across Active/Standby or Active/Active Appliance
126	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL Connection mirroring for SSL connections that are terminated/offloaded on the Server Load Balancer . Hence old connection should not fail or forced for SSL renegotiation esp for applications for which the server load balancer is doing SSL offloading.
127	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability
128	the solutiuon should support Unified Anti-Bot Detection and Protection & Cloning Application Traffic

129	WAF should support for future requirement to protect Credential Attacks Protects against attacks that can steal credentials from the user's browser, from data in transit and/or from the server without installing any agent at client machine
130	Support Building Customized business logic and Mitigate Zero Day Attack using Scripting
131	Should Support Behavioural DDOS Engine to Mitigate any L7 Attacks on the application
132	Should Support Automatic Signature Creation in case of BDDoS
133	The solution should support Brute Force Attacks Filter for Login Stress & Credential Stuffing functionality on day one
134	The proposed WAF should support ICAP, the security protocol for sending and receiving uploaded files for antivirus scanning from day one
135	The proposed solution shall support both positive and negative security model and work in HA mode with TCP, SSL mirroring of the traffic that is offloaded on the appliance and persistence mirroring, so that user session shall not be disconnected after failure of primary device. It shall improve the users experience.
136	System must support TCP optimization, TCP Buffering, TCP Connection Multiplexing to enhance protocol performance
137	WAF solution should have capability to support Anti-Bot Mobile SDK to whitelist and establish trust based on an embedded software package within the mobile application code, and corresponding cookie verification from day one.
138	Supported 3rd Party Repudiation Database which include Blacklisted IP Address, TOR, System Vulnerabilities, Country, Bad Proxy , Spam Source, Mobile Threats etc.
139	The offered product shall be resilient enough to mitigate following types but not limited to the following L7 DOS attacks GET Flood, SLOWLORIS,RUDY etc.
	Device Management, Reporting and Dashboards for WAF
140	The proposed Reporting solution must be a dedicated separate central management & reporting solution HW/Virtual to manage WAF Appliances centrally on Day One
141	The Platform must be able to allow the enterprise to measure infrastructure performance as it relates to application delivery, and to factor that application performance data into business intelligence tools such as troubleshooting, ROI calculations, and capacity planning.
142	The Proposed Management and reporting Platform must be able to provide tools for monitoring applications across the entire Application delivery network. E.g dashboard displays system statistics in selectable graphs, gauges, and tables. In addition to the pre-defined views, you can create custom combinations of the dashboard windows, and save them in groups. You can combine windows from different software modules in a single view, or use just the windows you want for a single module. Windows are available only for those modules that you have licensed and provisioned.
143	The Proposed Management and reporting Platform must be able to support historical statistics collection on CPU and memory usage, connections, and throughput in an easy-to-read graphical view and displays real-time historical stats by the hour, day, week, or month from the web dashboard GUI. In addition to real-time stats, historical trending reports must be viewed by hour, day, week, or month. E.g. view "real-time" profile and CPU usage statistics for individual virtual servers and "real-time" CPU and memory usage statistics for individual modules.
144	The Platform must be able to support Network Map of the virtual server IP addresses and server pools.

145	The Platform must be able to provide aggregated application visibility and reporting tools at the application level. This include viewing of detailed statistics about application traffic running through the system.
146	The Platform must be able to provide real-time application performance statistics, and diagnostic and troubleshooting information such as application response time, network latency, and connection statistics for the entire application, virtual servers, pools, and nodes.
147	The Platform must be able to provide user-created custom statistics that can be built on-the-fly by preconfiguration or predefined for more granular data and control through scripting or command shell. This is a mechanism for tracking information like metrics such as connections, data rates, etc.
148	The Management Platform should be able to perform device discovery and monitoring: Discover, track, and monitor up to 5 devices from day one—whether physical or virtual, both on-prem and in the cloud.
149	The Management Platform should have fine-grained Roles-Based Access Control (RBAC) which allows administrators to define roles and assign fine-grained control over configuration objects and tasks to those roles. Fine-grained RBAC uses the security principle of least privilege to ensure that a user has precisely the amount of privilege that is necessary to perform a role.
150	The Management Platform should support License Management via API and should be able to deploy and execute scripts on its managed devices remotely.
151	The Management Platform should be able to perform SSL Certificate Management; deploy, renew, or change SSL certificates. Receive timely alerts before certificates expire.
152	The Management Platform should be able to centrally manage Certificate Revocation Lists (CRLs).
153	The Management Platform should have utility license usage reporting: Enable utility licensing of its managed devices by generating and delivering reports of device use over time.
154	The Management Platform should be able to support and monitor device cluster: Monitor high availability (HA) and clusters for its managed devices and should have the option to take a backup before and after a device upgrade.

SOR-B: Backup Solution:

SN	Minimum Technical Specifications
1	Solution should be Appliance based with local storage and software.
2	Solution must offer change detection and an incremental approach to backing up data that changes over time.
3	Solution must offer Global, Inline, Block-Level, Source- and Target-Based deduplication across all a customer's data sources.
4	Solution must support Guest-Level Virtual Environments including Citrix XenServer, Kernel-based Virtual Machine (KVM), Oracle VM and Red Hat Virtualization
5	Solution Must support Host-Level Virtual Environments Including VMware vSphere, Microsoft Hyper-V
6	Solution must support back agents Including Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux and macOS
7	Solution should offer Offsite Replication Including Remote Physical Appliance, Remote Virtual Appliance without any Additional License or Cost
8	Solution should offer site-to-site replication without any additional License or cost

9	Solution must support Advanced sharing of different media across the environment (disk, tape and optical).
10	Solution must offer minimum 256 bit encryption for data being sent offsite and must store that data in an encrypted state. Data should be transmitted using a secure 256 bit encrypted protocol.
11	Solution should offer rate limiting for data sent offsite to limit the impact of replication on critical Internet resources.
12	Data stored offsite should be deduplicated and compressed to minimize impact on customer bandwidth and storage needs.
13	Solution should be able to access data from a variety of operating systems including Microsoft Windows, Linux, Unix, and Mac OS.
14	Solution should offer native support for MS Exchange backup and restore and recovery database restore option.
15	Solution should offer message level backups for MS Exchange and allow for restore of individual messages or entire folders.
16	Solution should offer backup task automation that allows multiple backups to be run each day.
17	Solution should provide automated notifications of backup success and failures, device availability, and alerts for critical system errors.
18	Solution must support GUI with centralized management / Single interface for management of all backup and archival activities.
19	Solution must support Advanced sharing of different media across the environment (disk, tape and optical).
20	Solution must support multiple level of backups including full, incremental and differential backups including the Virtual backups
21	Solution must support following application and database backup without CLI and without the requirement of temporary disk space for Oracle, 64-bit Active Directory, MS SQL, MS Exchange, Share-Point, MySQL etc.
22	Solution must be able to perform Source (Client) & Target (Backup Server) base block-level de-duplication without requiring expensive and proprietary disk appliances.
23	Solution should provide functionality to protect remote branch offices that ensures that data transfer across WAN links is minimized, providing both deduplication or byte-level replication options, whilst providing for granular restore capabilities
24	Solution must support various Encryption options (algorithms like 128 Bit AES, 256 Bit AES etc.) and encryption granularity and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.
25	Solution should integrate with Disk Backup target device which supports hardware/software data deduplication capabilities.
26	Solution must be able to auto discover Virtual Machines and dynamically configure them for data protection. It should not be any staging area requirement for virtual machine backup
27	Solution should offer flexible time-based retention options and version control that does not restrict the number of revisions or the time period in which data can be saved.
28	Solution should offer a full system or image based recovery option.
29	Solution should have a user interface that can be accessed from anywhere and can support management of multiple appliances at multiple locations.
30	Solution should include unlimited agent software licenses at no additional cost.

31	Solution should offer automatic software updates and access to new features included with annual subscription.
32	Solution should support rapid/instant VM recovery with LiveBoot for Vmware and Microsoft Hyper-V
33	Solution should have capabilities of recovering Granular file for VMware and Hyper-V.
34	Solution Should have 48TB of Usable Capacity with HW RAID 60
35	Appliance Should have 2 x 10Gb RJ45 or 2-port SFP+ Network Interface
36	Appliance Should have Hot Swappable Disks, In case of failure , individual drives can be replaced without impacting any other drives
37	Appliance Should have Hot Swappable Redundant Power Supplies and fans
38	Appliance shall have a minimum of 12 cores, 2.0 Ghz with dual Intel E5 based CPUs.
39	Appliance should have 64 GB or more memory.
40	The Overall Solution should have 3 yrs. Of NBD Warranty and 24x7 TAC Support.

SOR-C –i -Virtual Firewall:

SN	Minimum Technical Specifications
1	The solution should be virtual appliance based and enterprise class (complete control from GUI as well as CLI)
2	Proposed Firewall should support Hypervisor like VMware, KVM
3	The virtual appliance should support at least 6 Data vNICs
4	Firewall should support stateful inspection throughput of 1 Gbps with IPS
5	The solution appliance must have separate SYNC and management ports other than the above mentioned ports
6	The solution appliance should have a on device storage of min 50GB to be able to run OVA file and to hold multiple OS images, logs, backups etc
7	Firewall should support 10,000 new sessions per second
8	Firewall should support 100,000 concurrent sessions
9	Firewall should support at least 50 vlans
10	Firewall should operate in Route mode and transparent mode
11	The proposed system should have integrated Traffic Shaping / Rate-Limit functionality.
12	Certified by ICSA 4.1x OR EAL4 OR NDPP
13	The system should inherit all the standard RFC's.
14	Firewall should be either IPv6 Ready Logo certified or equivalent
15	Should facilitate to apply policy like Traffic shaping / Rate-Limit & policy based routing decision
16	User authentication facilitated by services like LDAP and RADIUS/AD.
17	Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
18	Management access control using Profile/Role based for granular control.
19	Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.
20	Support configurable option for E-mail or SMS alerts (Via SMS gateway) incase of any event trigger.
21	Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.
22	All SNMP versions support (v1, v2c and v3).

23	Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 50 VLANs
24	Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, BGP with IPv6), Static Route, Policy Based Routing, Multicast Routing
25	Support DHCP relay, DNS client and NTP client
26	Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice versa).
27	The appliance based security platform should be capable of providing firewall and VPN (both IPSec) functionality.
28	Intrusion Prevention System
29	The IPS capability should have NSS, ICSA or other equivalent Certification
30	IPS throughput should be atleast 1 Gbps or better for real world/production throughput
31	The IPS detection methodologies should consist of:
32	a) Signature based detection using real time updated database
33	b) Anomaly based detection that is based on thresholds
34	The IPS should be able to inspect SSL sessions by decrypting the traffic
35	The IPS system should have at least 7,000 signatures with support for custom IPS signatures
36	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
37	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
38	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
39	Solution should be able to detect & Prevent the Bot communication with C&C
	User Authentication
39	The proposed solution shall be able to support various form of user Authentication methods simultaneously , including:
	a) LDAP server entries
	b) Native Windows AD (Single sign on capability)
40	Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.
	High Availability
41	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one
42	High Availability feature must be supported for either NAT/Route or Transparent mode
43	High Availability Configurations should support Active-Standby.
	Management, Logging and Reporting
44	The management solution must offer console capability for managing the logs, policy, reporting and various features of the solution.
45	Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)
46	Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logsto syslog server and sending schedule reports and send via email.
	Support and Warranty
47	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.

48	Online upgrade the version of firmware/software/patches as and when required.
49	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
50	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
51	All the technical specifications mentioned above must be available from day one
	Other Requirements
52	For all requirements listed above, the necessary cables, connectors, external software media, manuals or any other hardware and software must be provided along
53	The solution must be present as Latest Leaders in Gartner's Enterprise Firewall Magic Quadrant.

SOR-C –ii - UTM:

SN	Minimum Requirement Description
1	The solution must be present as Leaders in latest Gartner's Magic Quadrant for Enterprise Firewall
2	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)
3	UTM appliance should have at least 04 x 10/100/1000 GE RJ45 ports and 4 x 1GE SFP ports with fully populated from day one
4	UTM appliance must have separate SYNC and management ports other than the above mentioned ports.
5	Firewall should provide at least 4 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.
6	UTM/NGFW appliance should have at least 32 GB RAM or higher
7	UTM appliance should have a on device storage of min 200GB to be able to hold multiple OS images, logs, backups etc
8	Firewall should support 20,000 new sessions per second or more
9	Firewall should support 2 Million concurrent sessions
10	The UTM appliance should be Rack Mountable, not exceeding 1U with redundant power supply fully populated from day one and should have hot-swappable fan tray/module
11	The Firewall solution should support NAT64, DNS64 & DHCPv6
12	Firewall should operate in Route mode and transparent mode
13	The appliance should support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability
14	The proposed system should have integrated Traffic Shaping / Rate-Limit functionality.
15	Support multiple firewall domains/instants/context /zone or more
16	Certified by ICSA 4.1x OR EAL4 OR NDPP
17	Internationally accepted marked/Certified like RoHS, UL/CUL, FCC,CE,..etc.
18	The system should inherit all the standard RFC's.
19	Firewall should be either IPv6 Ready Logo certified / FIPS/ USGv6 or equivalent
20	Should facilitate to apply policy like IPS, Content filtering, Traffic shaping/Rate-Limit & policy based routing decision
21	User authentication facilitated by services like LDAP and RADIUS/AD.
22	Management over GUI using HTTPS or equivalent secure mechanism, SSH and console access.
23	Management access control using Profile/Role based for granular control.

24	Configuration backup and restore on to/from a remote system via GUI/CLI over HTTP/SSH/TFTP or equivalent.
25	Support configurable option for E-mail or SMS alerts (Via SMS gateway) incase of any event trigger.
26	Firmware/OS/software updates via Web UI / TFTP or equivalent and should support version roll back functionality.
27	All SNMP versions support (v1, v2c and v3).
28	Support IEEE 802.1q (VLAN Tagging) and VLANs on all interfaces with at least 1024 VLANs
29	Dynamic Routing (RIPv2, OSPF, OSPFv3, BGP4, BGP with IPv6), Static Route, Policy Based Routing, Multicast Routing
30	Support DHCP relay, DNS client and NTP client; Firewall as security appliance should not use DHCP and should have static ip address
31	Support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT and IPv6 to IPv4 (vice versa).
	Intrusion Prevention System
32	The IPS capability should have NSS, ICSA or other equivalent Certification
33	The IPS detection methodologies should consist of:
	a) Signature based detection using real time updated database
	b) Anomaly based detection that is based on thresholds
34	The IPS should be able to inspect SSL sessions by decrypting the traffic
35	The IPS system should have at least 25,000 signatures with support for custom IPS signatures
36	IPS Signatures should be updated in different ways: manually, via pull or push technology. Administrator should schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available
37	IPS signatures should have a configurable actions like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident
38	Signatures should have severity level defined to it so that the administrator can understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)
39	Solution should be able to detect & Prevent the Bot communication with C&C
	Web Content Filtering & Application Control Features:
40	URL database should have at least 200 million+ sites and 50 + categories.
41	Support for geographical based filtering like country level TLD etc.
42	The appliance should have 3000 or more application signatures database
43	Should have the intelligence to identify & control of popular IM & P2P applications like KaZaa, Bit Torrent, Skype, You Tube, Facebook, LinkedIn etc.
	User Authentication
45	The proposed solution shall be able to support various form of user Authentication methods simultaneously , including:
	a) LDAP server entries
	b) Native Windows AD (Single sign on capability)
46	Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously.
	High Availability
47	System should have built-in high availability (HA) features without extra cost/license or hardware component from day one
48	Should support state full session maintenance in the event of a fail-over to a standby unit.
49	High Availability feature must be supported for either NAT/Route or Transparent mode
50	High Availability Configurations should support Active/Active / Clustering, Active/ Passive

	Management, Logging and Reporting
51	The system would be managed centrally using a web-based console that allows system monitoring, software updates, client configuration.
52	The management solution must offer console capability for managing the logs, policy, reporting and various features of the UTM.
53	Logging and Reporting up to layer 7 traffic details (firewall policy level, denied traffic details etc.)
54	Should provide log report in Web/GUI /dashboard based format with detailed information categorized by IP/Application/Port/Protocol etc., able to forward logsto syslog server and sending schedule reports and send via email.
	Anti-virus, Anti-bot & Advance Persistence Threat Solution
55	Should provide protection against zero-days, Trojan, worms or any other malicious content in traffic like SMTP, SMTPs, POP3, POP3s, IMAP, IMAPs, HTTP, HTTPs, FTP, FTPs etc. and must be configurable/applicable on specific firewall Policy
56	Remove buffering, it will introduce latency and impact user experience. All gateway level solution are flow
57	Should have option to respond to malicious detection like delete/quarantine the file or block the connection and send notification via e-mail/SMS.
58	For antivirus based solution AV signature database of proposed solution should comprise of up to date list of signatures of virus, malwares, spyware etc and other
59	Should be able to block or allow oversize file based on configurable thresholds
60	Firewall must include Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers also.
	Support and Warranty
61	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
62	Online upgrade the version of firmware/software/patches as and when required.
63	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
64	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
65	All the technical specifications mentioned above must be available from day one
	Other Requirements
66	For all requirements listed above, the necessary cables, connectors, external software media, manuals or any other hardware and software must be provided along

SOR-C –iii – Firewall Manager:

SN	Minimum Specification requirement
1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
2	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted
3	The management appliance should have 2 x 1G port and integrated redundant power supply from day one
4	The management platform must be able to store record of 15000 user or more
5	The management platform must provide a highly customizable dashboard.
6	The management platform must domain multi-domain management
7	The management platform must provide centralized logging and reporting functionality
8	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows

9	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
10	Should support troubleshooting techniques like Packet tracer and capture
11	Should support REST API for monitoring and config programmability
12	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
13	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
14	The centralized management platform must not have any limit in terms of handling logs per day
15	Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one
16	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
17	The management platform support running on-demand and scheduled reports
18	The management platform must risk reports like advanced malware, attacks and network
19	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.
20	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.
21	Online upgrade the version of firmware/software/patches as and when required.
22	Telephonic support with call logging mechanism should be provided on 24x7x365 basis.
23	Provide confirmation letter for license (if any) subscription for 3 years. License applicable from day one.
24	All the technical specifications mentioned above must be available from day one
25	Solution should be able to manage vFirewall and UTM mentioned in SOR

SOR-D-i – SOC:

SN	Detailed Technical Specifications
1	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018
2	The solution must address all major SIEM use cases including:
2.1	Log management
2.2	Incident investigations and workflow
2.3	Forensics
2.4	Security and compliance reporting and visualizations
2.5	Real time monitoring and alerting
2.6	Ability to do cross-data source correlations to detect specific patterns
2.7	Long-term data retention
3	The proposed solution should be able to handle 10,000 sustained EPS & 5000 Flows/sec from day one and scalable to 80,000 EPS.

4	The solution should be capable of supporting an increase in EPS capacity (i.e. beyond 80,000 EPS).
5	The proposed solution should be horizontally scalable to support increase in EPS and should have global corelation capability on raw or metadata/ normalized events (i.e. corelation of events on multiple hardware/appliances)
6	The solution should be capable of supporting enhanced storage capacity in future.
7	The solution should support increase in the user, EPS licenses as and when required in future.
8	The system should support integrating more organisations in future.
9	The Bidder will give the hardware sizing for the EPS count required since the solution is software based.
ADMINISTRATION AND CONFIGURATION	
1	The Security Intelligence solution must provide central management of all components and administrative functions from a single web/console based user interface. It should allow users to configure all features, backup configurations and push software updates etc. using one centralized interface.
2	The administrator must be able to define role base access control for controlled user and API access to the system by device, device group or network range. This includes being able restrict a users and API access to information to only those systems from a specific group of devices or network range. It also includes restricted access to specific data sources, data types, time periods, specific views, reports or dashboards.
3	The administrator must be able to define role based access to various functional areas of the solution. This includes being able to restrict a users access to specific functions of the solution that is not within the scope of a users role including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing.
4	The solution must support auto discovery of assets that are being protected or monitored and automatically start accepting events without any administrator intervention through an agent less solution.
5	The solution should support automated classification of assets that are being protected.
6	The solution must support the detachment of selected dashboards from the UI for use in SOC or NOC deployments.
7	The vendor of the Security Intelligence solution should provide and foster community oriented information and experience sharing among users of the security intelligence solution.
8	The solution should support the ability to modify communications ports between components from a central location.
9	The solution must provide an open API, ODBC or other method for access to data stored within the SIEM information database(s).
10	The solution must provide the ability to encrypt communications between components such as encrypted transmission of log data from device to SIEM system.
11	The solution must integrate with 3rd party directory systems as an authentication method such as LDAP,AD etc. for access provisioning to the SIEM system.
OPERATIONAL REQUIREMENT	
1	The solution must enable a phased role out of log management and security intelligence functions. Introduction of more analysis capabilities should minimize the need for additional system components and be enabled through license key upgrades.

2	The solution may provide a framework for future expansion and integration with other 3rd part solutions.
3	The solution must demonstrate ease of use. Ease of use is critical to the successful deployment and on-going use of the solution.
4	The solution must support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated.
5	The solution must support a webbased GUI for management, analysis and reporting.
6	The solution should support high availability requirements in an embedded fashion at all layers including collection, normalization, correlation and management and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.
7	The solution must ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., management console goes off-line all separate collectors still continue to capture logs).The retention, deletion, synchronization with SIEM data store should be automatic but it should be possible to control the same manually.
8	The solution should have an automated backup/recovery process.
9	The solution must automate internal health checks and notify the user when problems arise.
10	The solution should provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system.
11	The solution must deliver sample dashboards out of the box (i.e. for threat management, compliance management, etc.).
12	The solution should deliver customizable dashboard widgets that can present relevant security information to the users of the system (i.e. event views, network activity views, incident views, etc.).
13	The solution must maintain an externally accessible store or database of all assets discovered on the network. This asset data should include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database.
14	The solution must have the ability to maintain original time stamps for each event, and handle timestamps from different time zones.
15	The solution must have the ability to create indexes and data stores summarizing raw machine data, and then run searches/reports on these summaries for faster performance
ARCHITECTURAL REQUIREMENT	
1	The solution must enable deployments as software and/or appliance with a clear physical or logical separation of the collection module, logging module and analysis / correlation module with customization capability having provision for adding more devices, locations, applications, etc
2	The soution must install on major operating systems
3	The solution must installs on commodity hardware of our choice
4	The solution must provide browser-based UI access for end users (does not require thick client)
2	The solution must integrate with other security and network intelligence solutions.

3	The Security Intelligence solution must allow for customization to meet our unique requirements.
4	The solution must easily expand to support additional demand.
5	The solution should support a distributed database for event and network activity collection such that all information can be access from a single UI.
6	The solution should ensure the integrity and availability of the information collected.
7	The solution must provide intuitive mechanisms for troubleshooting such as proactive notifications, command line utilities etc.
8	The solution may support a distributed model for correlation such that counters, sequences, identity lookups, etc are shared across all collectors. (i.e., look for 25 login failures from the same user name followed by a single successful login for that same user name, where events seen by a single collector do not exceed the threshold of 25, but across multiple collectors would exceed the threshold).
9	The solution should support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a failed called SpecialID from my Custom Application).
10	The solution must allow for custom defined tagging of events.
11	The solution should provide transparent retrieval, aggregation, sorting, filtering and analysis of data across all distributed components.
12	The system should support Network Time Protocol version 3 for time synchronization.
13	The solution must support Disaster Recovery.It should have the provision to run in active / passive mode in a DC-DR environment and should be able to failover to automatically DR in case of a primary failure.
Security and Data Integrity of SIEM	
1	The solution should provide integration to enterprise single sign-on solutions enabling pass-through authentication of third party credentials
2	The system must provide Real-time remote indexing of data to minimize the opportunity for alteration of audit trails on compromised hosts
3	The solution should provide secure data stream access and distributed functionality via SSL/TCP
4	The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data
5	The solution must provide event hashing at index time to determine at search time if events have been tampered with
6	The solution must monitors its own configurations and usage to maintain a complete, digitally signed audit trail of who is accessing the system, what searches they are running, what reports they are viewing, what configuration changes they are making, and more.
LOG MANAGEMENT REQUIREMENT	
1	The solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage.
2	The solution may support log archives on 3rd party storage.
3	The solution should provide capabilities for efficient storage and compression of collected data.

4	The solution must support industry log collection methods (syslog-UDP (as detailed in RFC 3164) and TCP (as detailed in RFC 3195),DNS,DHCP, WMI, JDBC, XML,CSV,JSON,SNMP, Checkpoint LEA,FTP,S/FTP,ODBC,SDEE,Window event logs-agent based and agent less etc.,mail server, web server),directly pointing to log files over the network or on the indexer,Custom inputs which includes scripted and modular inputs, vendor supplied universal agents.
5	All logs should be authenticated, encrypted and compressed before transmission.
6	The solution should provide agent-less collection of event logs whenever possible.
7	The solution may provide the ability to distribute both event storage and processing across the entire Log Management/SIEM deployment.
8	The solution should support longterm access to detailed security event and, if available, network flow data. The system should be able to provide access to at least x months worth of detailed information.
9	The solution should capture flow information from multiple network points. Solution should support Network traffic collected via TAP, SPAN, and/or Mirror.
10	The solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs.
11	The solution should support heterogeneous devices/ applications and wherever required the bidder should develop customized software for log collection at no extra cost within the stipulated time.
12	The solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service
13	The solution should ensure optimum usage of bandwidth from remote locations to Central location with minimum overall load on bandwidth.
14	The system should identify the source while capturing event data
15	The system should be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.
16	The solution should be able analyse logs with different event formats e.g. well-structured logs, natural language logs, multi-line logs etc.
LOG NORMALIZATION AND CATEGORIZATION	
SN	**Requirement**
1	The solution must normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network.
2	The solution may provide a common taxonomy of events.
3	The solution must provide the ability to store/retain both metadata/normalized and the original raw format of the event log for forensic purposes.
4	The solution may provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields.
5	The solution should support/normalize event time stamps across multiple time zones.
6	Traceability of logs should be maintained from the date of generation to the date of purging.
7	The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. E.g.: The categorization may by be HIGH, MEDIUM, LOW or color coding.
EVENT FILTERING AND ANALYSIS	
1	The solution must provide near real-time analysis of events.

2	The solution must provide long term trend analysis of events.
3	The solution must provide the ability to aggregate and analyze events based on a user specified filter.
4	The solution should provide more advanced event drill down when required.
5	The solution should provide a real-time streaming view that supports full filtering capabilities.
6	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events.
7	The solution must support and maintain a history of user authentication activity on a per asset basis.
8	The solution should support user login concurrently for analysis as well as administration activities. The solution should support minimum 10 concurrent users from day one.
9	The solution should provide a user interface which allows analysts to manually analyze the data collected.
10	Analyst should be able to easily and quickly parse/ visualize/ analyze the normalized and raw data both from the online data store or the archived data store.
11	All logs that are collected should be studied for completeness of information required/ reporting/ analysis and requisite data enhancement should be performed to meet the reporting/analysis needs
12	The solution should be able to part and filter logs before storage on the basis of type of logs, date etc.
13	It should be possible to define purging and retention rules for log storage.
14	The solution should allow creating and saving of ad hoc log queries on logs. These queries should be able to use standard syntax such as wildcards and regular expressions.
15	The solution should provide bi-directional integration with 3rd party trouble ticketing/help desk or Incident Response Platform that security operations staff may use to guide their work
REPORTING	
1	The solution should provide reporting on all items available for management via the GUI.
2	The solution should provide configurable reporting engine for customized report, historical trend report, compliance report creation or 3rd party reporting integration.
3	The solution must support the ability to schedule reports.
4	The solution should provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues.
5	The solution should provide canned out-of-the-box reports for typical business and operational issues.
6	The solution should provide canned out-of-the-box reports for specific compliance regulations (PCI, GLBA,HIPAA,NERC,SOX, FISMA) and control frameworks including (NIST, CoBIT, ISO,SSAE).
7	The solution must provide a Dashboard for quick visualization of security and network information.The Dashboard design for the solution should be user configurable
8	The solution must support the automated distribution of reports.
9	The solution must support the capability to provide historical trend reports.
10	The solution must support the ability to centrally deliver vulnerability reports.
11	The solution may support the ability to centrally deliver asset reports.

12	The solution should enable the easy creation of a wide range of visualizations (not limited to fixed, pre-canned reports)
13	The solution should include following native visualizations:
13.1	Tables
13.2	Time charts
13.3	Line charts
13.4	Bar charts
13.5	Area charts
13.6	Pie charts
13.7	Scatterplot charts
13.8	Radial, filler, and marker gauges
13.9	Geo-IP maps
14	The solution's visualizations should have the ability to update in real-time
15	The solution's visualizations should be able to make clear outliers/anomalies in need of further investigation
16	All solution's visualizations should support drill-down, click-through capabilities to get from summaries to raw events within seconds
17	The solution's should have drag and drop user interface to enable non-technical and technical users to build complex reports without having to use search commands or understand the format of the underlying raw data
18	The solution should have ability to easily change titles, legends, and axis labels and settings for all charts
19	The solution should support easy “drag and drop” editing of dashboard panels
20	The solution should have the ability to easily print events, tables, and visualizations
21	The solution should have the ability to convert dashboards into PDF files and schedule them to be emailed to others
22	The solution should have the ability to integrate with external visualization frameworks and options (D3, Tableau, etc) for additional visualizations
23	The centralized web based/console user interface should drill down on reports and incident alerts on real time basis with full filtering and sorting capabilities.The solution should have drill down functionality to view individual events from the dashboard on events and find the IP addresses and geo-locations from the sources of suspicious or malicious IPs.
24	The solution should provide customizable management console/dashboard which can be provided to different stakeholders. Access to the solution should be restricted based on the role as identified and should be configurable.
25	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a report customisation tool for generation of any ad-hoc reports.
26	The solution should allow for qualification of security events and incidents for reporting purpose. The solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/ incidents.
27	Dashboard should display asset list and capture details including name, location, owner, value, IP address, platform details
28	Dashboard should capture the security status of assets and highlight risk level for each asset.
29	Dashboard should support different views relevant for different stake holders including top management and operations team

30	Dashboard should support reporting for consolidated relevant compliance for ISO 27001 regulatory requirements.
31	Dashboard should support export of data to multiple formats including CSV, Excel, PDF
32	Dashboard views should be customizable as per user rights and access to individual components of the application.
33	Administrators should be able to view correlated events, real-time raw logs and historical events through the dashboard.
34	The dashboard should permit setting up geographical maps/images on real time basis to identify impacted areas and sources of alerts. Geospatial capability and necessary database, updated regularly.
Open Platform	
1	The solution must offers a REST API to expose all indexed data, search commands, and functionality to external systems, applications, or dashboards
2	The solution must offers multiple SDKs written on top of the API for:
2.1.	Python
2.2.	Java
2.3.	JavaScript
2.4.	PHP
2.5.	Ruby
2.6.	C#
3	The solution should offers hundreds of free, public Apps for point products or use cases to create more value and accelerate time-to-value
4	The solution must provide system configurations to be configured via the UI, CLI, or files on the file system, enabling granular changes and customization
5	The solution's reports and dashboards should be editable either via the UI or underlying XML files, enabling flexible editing
6	The solution should have ability to easily forward on data to any external system or logging tool
6.1.	The soution should have the ability to forward raw data as syslog via TCP or UDP, or as raw TCP at index time.
6.2.	The solution should forward selected, transformed, and/or enriched events as a file, or as syslog over TCP or UDP at search time.
7	The Solution must have machine learing capabilities.
Use Cases Beyond Security	
1	The solution must assist in following use cases due to indexed data leading to a high ROI and cross-department collaboration.
1.1.	Compliance
1.2.	Fraud
1.3.	IT Operations
1.4.	Application Management
1.5.	Web/Digital Intelligence
1.6.	Business Analytics
1.7.	Industrial Data and Internet of Things
2	The solution must support a single solution to support all the data needs of different users, roles, and departments across the organization
CORRELATION AND ALERTING	

1	The solution must provide alerting based on observed security threats from monitored devices.
2	The solution must provide the ability to correlate information across potentially disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases etc.
3	The solution must provide alerting based on observed anomalies and behavioral changes in network activity (flow) data.
4	The solution proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. a) Flow based threat Detection b) User Behavior analysis c) DNS data analysis.
5	The solution must provide alerting based upon established policy.(e.g., IM traffic is not allowed.)
6	The capacity for event correlation engine that is being proposed should be properly sized for the specified EPS.
7	The solution may support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc.
8	The solution should provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions
9	The solution should provide UI based wizard and capabilities to minimize false positives and deliver accurate results.
10	The solution must limit the presentation of multiple similar alerts.
11	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.
12	The solution must support the ability to receive and correlate against threat intelligence feeds from OEM, external 3rd party security data feeds (open source or commercial) (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution.
13	The solution may support the ability to correlate against 3rd party vulnerability scan results.
14	The solution should monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert.
15	The solution may provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base servers) to minimize false positives associated with poor asset classification.
16	The solution may support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes.
17	The solution must generate and alert when a new service appears on the network or when new assets appear where they shouldn't or are not planned.
18	The solution should support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one hour period of time.
19	The solution should provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity.

20	The solution must support Netflow, JFlow, SFLow collection and correlation.
21	The solution should be able to pull in identity context from variety of sources in order to appropriately map user identity with current activity. Solution should be able to map multiple user aliases/attributes back to a single user.
22	The solution must support correlated incidents for applications, databases, servers, networks etc.
23	It should be possible to apply correlation rules for real time events as well as historical data
24	The solution must be able to detect when strange users access a specific host, learn what users connect with specific assets such as a point of sale terminal and then alert when new users login.
25	The solution should provide summary of log stoppage alerts and automatic suppression of alerts.
SEARCH	
SN	**Requirement**
1	The solution must be able to do full-text search on any field in the indexed data based on:
1.1.	Keywords
1.2.	Time ranges
1.2.1.	Specific or relative time windows down to the month/day/minute/second
1.3.	Boolean logic (and, or, not, etc)
1.4.	Regular expressions
1.5.	Wild card syntax
1.6.	Statistical analysis including:
1.6.1.	Count of occurrences, distinct count of occurrences, sum
1.6.2.	Most common values or least common values of a field
1.6.3.	Minimum, maximum
1.6.4.	Average, mean, mode, median
1.6.5.	Standard deviation, variance
1.6.6.	The identification of anomalous values in results that may be irregular, or uncommon
1.6.7.	The statistical correlation between fields
1.6.8.	Clustering of events together based on their similarity to each other as a single event
1.6.9.	Truncate outlying numerical values in selected fields to assist in statistical correlation
1.6.10.	First and last seen value
1.6.11.	Percentile
1.6.12.	Predicted values (search that looks at historical data to mathematically predict future values)
1.6.13.	Perform a union, diff, or intersection of individual or multiple search results
1.6.14.	Search for relationships between pairs of fields by comparing the values of one field to a reference field and value pair
2	The solution must be able to do baselining and then apply the above search logic to find outlier/anomalies from the baseline that may be advanced, non-signature based threats
3	The solution must have the ability to data-mine based on who, what, when and where searches.
4	The solution must have th ability to save, share or modify searches.
5	The solution must have the ability to run the searches both in real time or

	scheduled.
6	The solution must have the ability to run multiple concurrent searches
7	The solution must have the ability to directly search raw data (using existing search capabilities) stored externally in Hadoop HDFS file systems and the results made available for advanced visualizations
8	The solution must have real-time alerting capabilities on a per-search basis that can:
8.1.	Send an email
8.2.	Add to a RSS feed
8.3.	Execute a custom script where scripts can act as “middleware” enabling automated remediation actions involving different vendor products
8.4.	Be throttled so not every event that meets the search parameters results in an alert action
9	The solution must not have any fixed maximum on the number of searches or alerts that can be run
10	Every additional sources of information integrated at later stages should be normalized into the same analysis workspace.
11	It should be possible to add any real time contextual information/ situational awareness data into the normalized data
12	SIEM must allow the creation of an unlimited number of new correlation rules
13	The solution should have the capability to identify which queries and indexes have been searched most to improve the query response time
14	The solution must have capability to query the stored event to detect such activity in the past.
15	Solution should have the ability to perform free text searches for events, incidents, rules and other parameters.
SIEM WORKFLOW	
SN	**Requirement**
1	The solution must provide ability to send notification of correlated alerts via well defined methods (i.e. SNMP trap, email, etc.)
2	The solution should provide embedded workflow capability that security operations staff can use to guide their work.
3	The solution should provide bidirectional integration with 3rd party trouble ticketing/help desk systems that security operations staff may use to guide their work.
4	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc..
5	The solution must provide a mechanism to annotate a security incident as it is addressed by the security operations staff.
6	The solution must provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). The user must be able to filter incidents along these defined attributes.
DATA SOURCE REQUIREMENTS	
SN	**Requirement**
1	The solution must support any human readable machine data from sources including but not limited to any app, OS, device, or system whether virtual/physical or cloud-based.

2	The solution must not be reliant on vendor-supplied, custom connectors to ingest data from different sources.
3	The solution must be “Future-proof” in that it can accommodate new data sources or changes in the log format of an existing data source
4	The solution must support information collected from Microsoft based servers and end-user systems.
5	The solution must support information collected from Linux/Unix based servers and end-user systems.
6	The solution must support information collected from mainframe servers.
7	The solution must support information collected from enterprise class database solutions.
8	The solution must support information collected from commercial applications (i.e. JD Edwards, SQL Server, Oracle, IBM DB/2 400, WebSphere, Web, etc.).
9	The solution must support information collected from Data Leak Protection (DLP) Security software and tools.
10	The solution may support information collected from proprietary applications.
11	The solution should support information collected for Database Activity Monitoring (DAM) Security software and tools.
12	The solution should support information collected from File Integrity/Activity Monitoring (FIM/FAM) Security software and tools.
13	The solution should support information collected from Identity and Access Management Security software and tools (IAM).
14	The solution must integrate with corporate directories (AD, LDAP etc.) to extract employee information including employee user names, first, last, phone, manager, department, location, if privileged, if on watchlist, start and end dates, etc.It should have ability to correlate multiple user names back to a single employee
15	The solution must integrate with asset center for asset information (e.g., CMDBs or other asset databases) for extracting asset information including device host name, IP, MAC, location, if containing confidential data, if relevant to a given regulation, etc. It should have ability to map an IP to a machine name and vice-versa
16	The solution must integrate with lists of prohibited services/ processes/ IPs/ ports/ protocols
17	The solution must support information collected from Network flows (i.e. Netflow, J-Flow, S-Flow etc.) products.
18	The solution should support information collected from network management systems (i.e. OpenNMS etc.).
19	The solution must support information collected from Network infrastructure (i.e. switches, routers, etc.).
20	SIEM should support Connector Development tool/SDK /API availability for developing collection mechanism for home-grown or any other unsupported devices/applications. The respective tool should be provided
21	The solution must support information industry leading vulnerability scanners.
INDEXING	
1	The solution must have ability to index all the original, unmodified data and make all of it available for both searches and reports
2	The solution should be able to index multi-line or complex event logs
3	The solution must support following Security sources that can be indexed:
3.1	Firewalls
3.2	Intrusion Detection System / Intrusion Prevention System

3.3	Authentication system (incl LDAP and Active Directory)
3.4	Data Loss Prevention
3.5	Anti-malware
3.6	Automated malware analysis tools
3.7	Web security or web proxy
3.8	Email security
3.9	Vulnerability scanners
3.10.	File integrity monitoring
3.11	Web application firewalls
4	The solution must support following Non-Security sources that can be indexed:
4.1	Operating system logs (endpoints and servers)
4.2	Email server
4.3	Web server
4.4	DHCP/DNS
4.5	VPN
4.6	Network Flows (NetFlow, IPFIX, etc)
4.7	PCAP files
4.8	Networking devices (routers, switches)
4.9	Databases and mainframes
4.10.	NAS devices and filers
4.11	Hypervisor and virtual machine logs
4.12	Service desk
4.13	Call records
4.14	Mobile devices and mobile device management systems
4.15	Server and Endpoint Management tools
4.16	SCADA devices
4.17	Industrial control systems
4.18	Manufacturing systems
4.19	Physical badge data
4.20.	Hosted VM environments (Amazon Web Services, Rackspace, etc)
4.21	Cloud-based applications (Box, Salesforce.com, etc)
4.22	Social media (Twitter, Facebook, Foursquare, etc)
4.23	Web analytics
4.24	ERP and CRM
4.25	RFID
4.26	GPS
4.27	Custom applications
5	The solution must have ability to directly connect to any SQL database table(s) and extract the contents for indexing
6	The solution must have ability to import raw data from Hadoop for indexing

Packet Capture:

SN	Minimum Requirement Description
1	Perform Full Packet Capture of network traffic with zero packet loss. Support the retrieval of relevant packets to a cyber security incident
2	Support importing archived PCAP files for analysis, Support importing other structured and unstructured content for analysis

3	Index all the data in the packets to simplify navigation across data silos and Enable search-driven data discovery of packet metadata AND content for incident analysis
4	Highlight potentially malicious or suspicious content,Allow for assigning security analysts to specific security incident investigations
5	The solution should have capability to integrate with SIEM to have unified visibility.
6	Solution should be sized for traffic rate of 1Gbps or higher.
7	The solution must have feature for root cause analysis and PCAP import while the System is performing LIVE packet capture of the network.
8	Anomaly Detection – find anomalous traffic patterns occurring in IT network
9	3rd Party Threat Feed integration – add feeds, like Snort, quickly and easily
10	Should be able to support integration with Endpoint Management/EDR solution for remediation endpoints via single agent EDR and Anti-virus solution.The AV and EDR must be from same OEM. Provided AV must be in leaders Gartner Quadrant.
11	Should have ability to filter, view timeline, or readily access Email and IM artifacts in one pane of glass
12	Should provide Regeneration and Playback functionality: Ability to create shadow networks. Regeneration and Playback: Point and click to instantly regenerate traffic (at configurable speeds) to a chosen NIC on a shadow network for further analysis in 3rd party systems. Without interruption of regular services.
13	Should be an on-premise appliance-based solution with capability to do packet capture, storage, protocol dissection.
14	The solution should support - classification from more than 3000 protocols/applications(natively without writing any custom parsers) and thousands of descriptive, metadata attributes, including content types, file names, and more - for easy analysis and recall without writing any custom parsers.
15	Ability to import PCAP & PCAPNG files simultaneously while the live capture is going on. making it easy to analyze historical data or, captures from other sources. The solution should also include a packet viewer that is capable of following TCP streams.
16	Should capture all packets from network in real time and be able to classify, extract and analytics, reconstructs network activity and forensics over IPv4 and, IPv6.
17	Root Cause Explorer Features - Automates tracing of HTTP referrer chains that can significantly reduce time to search for related preceding sessions.
18	Ability to create a new rules that applies to all previously captured data without the need to re-ingest older captured data to get the Application Rule to create a new piece of meta data
19	Should support Integration With Endpoint Detection and Response (EDR) technology as proposed in the RFP which should remediate and blacklist the suspicious/malicious files in entire network with one click from same console. The AV and EDR must be from same OEM and provided AV must be leader Gartner Qudarnt for last 3 years
20	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay, page reconstruction, image views, artifact & raw packet extractions.
21	Proposed solution should Integrate with On Premise Malware Sandbox Analytics solution. Security analytics should be able submit files for detonation and analysis.The ATP solution must be able to submit files for sandbox.
22	The solution should support network anomaly detection that performs statistical analysis on captured data and alerts on anomalous behavior. It should support pivot from the alert to an investigation view, where details around anomaly are available for analysts review.
23	The Solution must be configurable remotely by the administrator
24	Should capture signature/heuristics and behavioral based alerts and block the malicious activity
25	Should Identify the source of an attack
26	Solution must perform flow generation and analysis and must perform aggregation of all traffic pertaining to single session with a single flow records.

27	The Solution must maintain the integrity while sending SSL traffic.
28	Solution must support provision to implement custom environment.
29	Solution must identify every user connecting to the Network, record every conversation.
30	Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.
31	The solution should be able to provide suggested mitigation actions for events
32	Security Analytics should be proposed with required SSL visibility solution to enable meticulous network forensics and monitoring across all network traffic, thousands of applications, dozens of file transports, all flows, and all packets—including encrypted traffic. Should provide total visibility into network traffic with actionable intelligence so that department can quickly shut down exposure and mitigate ongoing risk. Should provide: • Detailed insights from all forensic captures • Establish policies to selectively decrypt SSL traffic • Share encrypted traffic insight with your security applications
33	Solution must support automatic visibility and interpretation of SSL decrypted traffic regardless of port or protocol. SSL decryption should be provided through the dedicated purpose built appliance based. There has to be integration with SSL decryption and security analytics solution.
34	The solution provided for SSL decryption must support 78+ Ciphers and TLS 1.3. The packet capyure tool and SSLVA must be from same OEM.
35	Should have minimum 6 x 1 GbE interfaces and 128 GB RAM.
36	Perform meta data extraction, meta- indexing, anomaly detection and data enrichment into Antimalware/Dynamic Analysis and various threat intelligence. Submit details on solution capability, what security threats it can detect and what it cannot detect without relying on any 3rd party tools
37	provide complete control over traffic capture filters, providing the ability to filter network traffic, either during capture or when replaying captured traffic later, inclusively or exclusively.
38	The Solution should include 3 yrs. Of Subscription.

SOR-D-ii & iii - Anti Virus + EDR (Client & Server):

SN	Minimum Technical Specifications
	General Requirements
1	The solution must be in Leader's quadrant of the latest Gartner Magic Quadrant report on End Point Protection
2	Solution must scan, detect, clean, delete and quarantine the infected files.
3	The solution would be managed centrally using a web-based console that allows system monitoring, software updates, client configuration, and event reporting. The central site administrator should have the ability to manage the software at all levels of the network and have the ability to remotely deploy product updates and modifications to all users.
	Client Side
4	The Bidder should include the Subscription for 3 yrs. For 1200 Devices.
5	The Product agent of the proposed Product system shall support Windows, MAC and Linux OS.
6	Solution must clean/ delete/ block malicious codes/software in real time, including viruses, worms, Trojan horses, bot, spyware, adware, mass mailing worms and Rootkit for Windows based Operating systems /Root kit along with webshell(s) for UNIX/Linux based operating systems
7	Solution must have capability to scan, detect and clean the boot sector and Master boot record
8	The anti-virus should provide protection for critical system by blocking blacklisted applications.

9	Solution must have embedded behavioural analysis and protection technology apart from signature based clean/delete/quarantine for unknown threats.
10	Solution must scan, detect and clean or delete malicious code for protocols like POP3 /IMAP/FTP etc.,
11	The anti-virus solution should prevent malicious applications from inserting code into trusted applications.
12	Solution must provide to install antivirus agent through various techniques like web based, MSI package or other methods in workgroup and Active Directory/LDAP environment.
13	The antivirus solution should provide scanning capabilities such as:
	On access scanning
	Real time scanning
	On-demand scanning
	Scheduled scanning
	Heuristic scanning
	Compressed file scanning
	Firewall
14	To address the threats and nuisances posed by Trojans, the solution should be able to do the following:
15	Terminating all known virus processes and threads in memory
16	Deleting any drop files created by viruses
17	Removing any Microsoft Windows services created by viruses
18	Includes Cleanup for Spyware, Adware etc
19	The solution should provide Role based administration.
20	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log
21	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.
22	Solution must provide to scan single file/directory/entire system and detect, clean, delete or quarantine the infected file.
23	Solution must provide scheduled scan configuration for full-disks scan at designated time from central manager for clean, delete or quarantine infected file.
24	Solution must provide to prevent endpoint users from uninstalling or disabling the managed antivirus services.
25	Solution must provide to exclude the specified files/directories from real time and manual scan.
26	Solution must provide a utility program for clean uninstallation process of the corrupted antivirus.
27	Solution must be fully IPv4 and IPv6 compliant (dual-stackable)
28	Solution must provide virtualized environment
29	Solution must provide Endpoint based Intrusion Prevention System to proactively block and safely eliminate malwares and potentially unwanted program from endpoints.
30	Solution must allow for creating whitelisting of application programs, DLLs and executable files and block all remaining programs, DLLs. executable files for execution.
31	Solution must provide to create classify applications which are attempting network access, and block unauthorized connections and data transfers by malicious programs.
32	Solution must provide to protect against zero-day attacks
33	Solution must provide all the supported versions/latest versions of Microsoft Windows Operating Systems.

34	Solution must provide to generate infected systems report with their source and destination IP address.
35	Solution must provide to generate malware, name-wise reports based on source and destination IP address.
36	After development of signatures for logs submitted for a suspicious system, analysis report must be submitted to RailTel. The Analysis report should contain IP address of the system, List of files found suspicious in the submitted log
37	Solution must provide to generate following reports:
	Current Virus Definition.
	Virus Definition updates.
38	Report generated must be exported to other applications like HTML, Microsoft Excel, CSV or PDF.
39	Graphical Charts for malwares, infected endpoints etc. for managed clients.
40	Solution must provide to send endpoint logs based on IP and MAC address automatically up to CMAS.
41	Solution must provide that the managed endpoints must send Antivirus event logs.
42	Solution must provide to send logs of device control and application control tothe central manager
43	Solution must provide that the managed endpoints must send Antivirus firewall logs i.e. compliance violations and access log.
44	Solution must provide that the managed endpoints must send Endpoint Based Intrusion Prevention System compliance violations and access log.
45	Solution must provide to integrate with 3rd Party Log Analyzer Application Software like Arc-Sight.
46	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.
47	OEM/bidder must provide RCA (Root Cause Analysis) report of technical problem/ incidence / issues reported and resolved.
48	Vendor must provide log analysis of infected systems and submit required suspected files to OEM lab for new signature
49	Vendor must provide software upgrades, new malware antivirus signatures, and technical know-how transfer training.
	Server Side
50	The Bidder should include the Subscription for 3 yrs. For 200 Devices.
51	The Product agent of the proposed Product system shall support both Windows and Linux OS server edition.
52	The solution should analyses all packets to and from the server for intrusion attempts and propagation
53	Server Security solution should have anti-malware, firewall, HIPS, Integrity monitoring within the Same Agent.
54	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems.
55	The solution should encompasses host-based firewall capability. Must allow definition of network-level filtering rules based on source and destination IP/network address, protocol, and source and destination ports in support of organizational security policy to allow/disallow specific types of activity between hosts
56	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers or provide attack prevention using the least privilege containment approach
57	Solution should offer protection for virtual or physical, or a combination of both the environment
58	Solution should be capable of blocking and detecting of IPv6 attacks.
59	The solution should provide protection for Web Server and Database Server

60	Solution should have the ability to lock down a computer (prevent all communication) except with management server.
61	The solution should protect against SQL injection attacks
62	The solution should have provision to protect against cross-site scripting (XSS) attacks
63	The solution should support system lock-down by blocking all the applications to run on the system. The administrator can create a white list of application so that only those applications are allowed to be executed
64	The solution should encompass a wide array of built-in alerting, blocking, and logging responses for each event and should provide an automatic alert to the system administrator on multiple virus detections.
65	The solution should support response adjustment on a per signature/policy basis.
66	The solution should have the option to block intruder for a particular period of time or should have targeted prevention policy to respond to server incursion
67	The agents shall be managed by a central administration system designed for large-scale enterprise deployments
68	The central site management system must be capable of providing a daily report of found viruses, including locations and a report of incomplete or failed nodes updates for each location. These reports must be accessible by the network administrator at the Central Server. Should be able to generate report data into a variety of different file formats like HTML, PDF etc.
69	Solution should have application control, HIPS, Anti Malware being installed on single server. No separate servers and agents should be required for HIPS or application control
70	Solution should have an emulator to cause threats to reveal themselves. This should not be a part of sandboxing and should run individually in each agent
71	Solution should have Deception component from same or different OEM which helps identify the unknown attacks that conduct file traversals, network discovery, terminate processes, try to conduct credential theft, and more
72	The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources
73	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 OS patches have been applied to the operating system.
74	If the host is non-compliant with the policies, the solution must automatically initiate remedial action, downloading and executing/inserting a software, running scripts , by setting required registries keys. The solution should recheck host for compliance after remediation and grant access for the compliant host to the network.
75	The solution must be able check whether required software, security patches and hot fixes have not been installed on the endpoint as mandated by organization, the solution should be set to connect to an update server to download and install the required software based on the policy.
76	The Solution should include 3 yrs. Of Subscription

SOR-D – iv - Vulnerability Assessment:

SN	Minimum Technical Specifications
	General Specification
1	The scanning solution must be Software / Appliance based, that is deployable in windows and Linux platforms

2	The scanner software / appliance must be hardened OS and very secure to ensure that the platform is not itself vulnerable.
3	The solution must support different platforms of OS like Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IBM
4	The solution must support Databases like Oracle, SQL Server
5	The solution must support scanning of different networking and security devices like routers, firewalls like CISCO, Checkpoint and Juniper for vulnerability and policy scanning
6	The solution must support scanning of Virtual hosts: VMware ESX, ESXi, vSphere, vCenter, Dockers for vulnerability and policy scanning
7	The solution must be able to perform vulnerability assessment of Wireless devices.
8	The solution must be manageable through a web based interface (GUI) which in turn can be accessed by users across the organization from different locations
	Signatures
9	The Signatures and threat feed database must auto update from the OEM facility
10	The Signatures must be configurable like severity modification, adding more intelligence or even disabling a signature.
11	The Signatures must be mapped to CVE ID, CVSS v2 and v3 scores.
12	The Signatures must have information about public exploit availability from more than 5 exploit DB's, Patch availability etc
13	The Signature database must be exportable to CSV, PDF etc
14	The solution must provide Real time threat information like easily exploitable, public exploit available, DoS, High lateral movement, High Data Loss, Actively being exploited etc
15	The solution must allow creation of custom signatures using OVAL etc
16	The Solution must automatically notify respective platform teams of new vulnerability for specific OS
	Scanning capabilities
17	i). Must support scanning of IPv4 and IPv6 devices/systems
	ii). Must allow scan bv hostname
	iii). Must use proper asset tracking like IP based, DNS or NetBIOS hostname based
18	The solution must Identify devices, Host OS, services accurately
19	The solution must perform authenticated scans and null session scans.
20	The solution must have minimal or no impact on Network traffic, server performance, network devices etc. during deployment and operation
21	The solution Must perform cross platform assessment with relevant audits.
	i). Must have intelligence to execute only relevant audits on the target
	ii). Must auto discard an IP that is not alive and move on to next available IP
	iii). Must provide data about time spent on scanning each asset.
22	i) The solution must be self updating including signatures and OS components
	ii) Scanner update must be automatic
	Exploit mapping
23	The Solution must automatically map a vulnerability to a known public exploit.
24	The Solution must perform automated Asset inventory and must be able to collect and allow searching via inventory details like
	i) Inventory of OS

	ii) Inventory of Certificates
	iii) Inventory of ports and services
	iv) Inventory of Applications
	v) Inventory of users on a system
	vi) Inventory of Hardware manufacturer for Host OS like workstations, Servers and laptops
	vii) Inventory of drives & file shares
25	The solution Must provide information about last scan date of an asset
26	The solution Must perform automated Asset inventory
27	The solution Must provide comprehensive asset discovery
28	Discover Net blocks / CIDR's
29	Discover new devices on the network
30	Discover what devices have been removed from the network based on delta
31	The solution Must provide a graphical, interactive and search friendly topology of the discovered assets
	Vulnerability Scan capabilities
32	The solution must have a Scan engine that must find vulnerabilities, ports, services, applications, certificates and users inventory
	i) This data must be searchable and reusable
	ii) The search query performed by user must not be a complex language
	iii) This data must be available in visual form on a dashboard, portlet, widget etc
33	The solution must have facility to configure Scans for performance, Maintenance windows , intensity, Host OS type and type of vulnerability
34	The Solution must send email / CEF alerts for Vulnerabilities, ports, services, certificates, software installed.
35	The Solution Must allow multiple scan jobs at the same time
36	The Solution Must allow Scanning exclusion by IP or range
	i) Allow Excluding IP's, IP ranges at scan launch
	ii) Allow a global exclude list to ensure scans never happen on those IP's
37	The Solution Must allow scan on targets defined dynamically
	i) Identify Web-Servers, databases, network devices,
	ii) Identify assets running specific OS
	iii) Identify assets running specific open ports
	iv) Identify assets running specific services
	v) Identify assets running specific application
	vi) Identify assets scanned / not-scanned in the last X days
	vii) Identify assets with a specific vulnerability or zero day
	viii) Identify assets with actively exploited vulnerabilities
	ix) Identify assets with EoL and obsolete software
38	The Solutions Scan engine must be able to include or exclude a specific list of signatures
39	The Solution must allow to choose a scanner device at time of scan
40	The Solution must group multiple scanners in one single large job automatically
41	The Solution must show scan progression and partial scan results in case of large scans

42	The Solution must be able to scan for SANS Top 20 vulnerabilities
	Reporting Requirements
43	The solution Must have inbuilt reporting templates
44	The solution Must allow custom template creation
45	The solution Must allow report distribution automatically and securely with a password
46	The solution Must allow various output formats like CSV, DOC, HTML, PDF, XML etc
47	The solution Must allow to report on an asset search condition based on asset attributes
48	The solution Must have graphical charts and graphs showing Vulnerabilities, severity over a time and trending information
49	The solution Must be able to Schedule Scanning.
50	Reporting and Schedules must be able to auto start, auto pause, auto resume and auto cancel to suit a maintenance window if required
51	The solution Must perform dynamic asset search based on asset parameters
	i) Search by OS, hostname, ports, services, vulnerability, application
	ii) Search by last scan date and first scan date
	iii) Search based on user accounts and time-zone
52	Solution should allow users to customize the dashboard
53	The solution Must allow integration with popular SIEM, IT GRC products like Arcsight, RSA, Nitro etc
54	The solution Must provide API responses in XML, CSV, PDF, JSON
55	Solution must allow multi factor authentication for secure login
56	Solution must allow settings for granular user role and permissions configuration
57	The Solution must have option for external authentication for AD integration
58	The Solution must provide inbuilt ticketing for vulnerability status monitoring
59	The Solution must provide a risk ranking system based on asset criticality
60	The Solution must have a vendor provided severity mechanism to aid when no CVSS is present
61	The Solution must identify the critical vulnerabilities to prioritize remediation
	i) Identify Easily exploitable vulnerabilities
	ii) Identify vulnerabilities with exploit kits available
	iii) Identify vulnerabilities with zero day
	iv) Identify Zero Day vulnerabilities
	v) Identify vulnerabilities with High Data loss potential
	vi) Identify vulnerabilities with high lateral movement
	vii) Identify vulnerabilities of type Malware, Trojans
	viii) Identify vulnerabilities with No path available
	ix) Identify vulnerabilities that result in DoS
	x) Identify vulnerabilities being used for Active attacks in the real world
	Scanner Requirements
62	The solution must have a function so that large scans can be auto distributed among all available scanners to finish a scan faster and efficiently.
63	The solution Scanner device communication with management console must be encrypted and compressed.

64	The solution must allow a way to have N level failover for scanners so that any available scanner picks up the job
65	The solution must alert via email automatically if one or more scanner devices are down
66	The solution in virtual appliance form must support Hyper-V/VmWare/Citrix/ESX/Oracle VM
67	Storage and retention capabilities
68	The Solution must allow reporting on historic data as long as 2 years or more
69	The Solution must have its own database for storage, no additional license cost must be required
	Warranty, Training & Software subscription:
70	VA vendor must have 24/7 security service
71	The solution must offers integrated password management integration with PowerBroker Password Safe as well as it includes a built-in third party password management connector.
72	The Solution must support Assess: Identify security gaps and vulnerabilities•Remediate: Prioritize what actions to take first•Comply: Automate risk and compliance assessments
73	The solution delivers asset auto discovery across network devices, servers, and databases and assesses the security configuration of assets
74	The solution must offers out-of-the-box, comprehensive coverage for 100+ regulations, frameworks, & best practices that are translated into questionnaires.
75	The solution must automates policy definition and policy life cycle management
76	The solution must aligns security and compliance operations with business priorities by defining risks according to business thresholds, by mapping risks to assets, controls and owners, and by calculating and aggregating risk scores
77	Solution must Support for REST APIs to enable integration and automation around commonly used functionality like assets, jobs and standards management
78	Solution must Support for offline data collection with agents to enable usage in air-gapped networks
79	The Solution should include 3 yrs. Of Subscription
81	1200 Desktop/ Laptop and 200 Servers Subscription/ Licenses should be part of the bid.

SOR-E- i- Rack Server:

SN	Component	Minimum Requirement Description
1	General Requirement	Server should be a vSAN certified ready node
		Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates, system drift detection and secure erase security features inbuilt.
		SAP Certification: Server should be SAP HANA certified.

		Inbuild Server Management i) Software should be from the same H/W OEM and should integrate with 3rd party vCenter and System Center, Nagios, CA management console etc. ii) Server Monitoring: Should be able to monitor all system health and systems components (CPU,RAM, HD, FANS, Power Supplies, BIOS, HBA's, NICs, CNA's) through dash board. iii) Power & Temperature monitoring: Should support Real-time power meter, graphing, thresholds,alerts & capping with historical power counters, Temperature monitoring & graphing through dashboard iv) HTML5 support for virtual console & virtual media without using Java or ActiveX plugins v) The servers should have dedicated secure Remote management port. vi) Server management console should work seamlessly with existing OpenManage server console
		Mounting of server in existing rack in Data center along with Power supply and Network cabling, installation and configuration of systems, physical connectivity to the switches via FC cables in RailTel Data center along with supporting cable for HCI configuration .
		Conducting Power On Self-Test (POST) of all compute Network and storage
		Basic server installation and management training to be provided by the OEM or Authorized distributor/Partner of OEM.
		Material required for Installation and commissioning of Servers and switches in Data center to be supplied by Bidder (Patch cords , patch cable connectors etc.)
2	Market position	The OEM for the proposed server must be in Leaders quadrant in the last two Gartner's report of "Magic Quadrant for Modular Servers".
3	Chipset	Intel C621 or higher
4	Form Factor	Max. 2U rack mounted with sliding rails.
5	Configured CPU	Should be populated with 2nos. of Intel Xeon Skylake CPU architecture, each CPU should be 16 core 2.3Ghz or more.
6	Memory slots	24 DDR4 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 2933MT/s. Optionally support up to 12 DIMM & 12 NVDIMM
7	Memory configured	**Configured with 128GB using 32 GB DIMM's** scalable to 1.5TB
8	Disks supported	Front drive bays: Up to 24 x 2.5" SAS/SATA/SSD,
9	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 4Gb cache
10	Disks configured	2 nos. of 240GB BOSS card or SATA/SAS SSD in mirrored configuration for OS & 3 nos. of 960 GB SSD SAS and 6x2.4 TB 10k rpm SAS drives.
11	DVD writer	DVD RW
12	I/O slots	Up to 6x PCIe Gen3 Slots
13	Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.
14	Softwares	Should support Vmware Vsphere & VSAN Enterprise Lic. Or Similar etc.
15	Certification and compliances	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES)
16	Power Supply	Platinum rated redundant Power Supply
17	SD Modules slots	Dual SD Module slots supporting redundant configuration
18	Management integration	Support for integration with Microsoft System Center, VMware vCenter

19	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping Temperature monitoring & graphing
20	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD.
21	Configuration & management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & CNA & system health • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile • Automated hardware configuration and Operating System deployment to multiple servers • Zero-touch repository manager and self-updating firmware system using AI/ML • Virtual IO management / stateless computing • Support for Redfish API for simple and secure management of scalable platform hardware • Server management system should provide anticounterfeit • The mgmt. solution should provide recommendation engine provides actionable intelligence for IT operations management. The insights should be driven by expert systems and best practices from OEM. • Server management system should provide an alert in case the system is not part of OEM Hardware Compatibility list
22	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins
23	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks
		Should protect against firmware which executes before the OS boots
		Should provide effective protection, reliable detection & rapid recovery using: - Silicon-based Hardware Root of Trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Automatic BIOS recovery - Rapid OS recovery - System erase
		Configuration upgrades should be only with cryptographically signed firmware and software
24	Intrusion alert	Intrusion alert in case chassis cover being opened.
25	Warranty	03 years On-site comprehensive warranty with 24x7x365 remote hardware support.

SOR-E-ii – 10G Switch:

SN	Minimum Requirement Description
	Solution Requirement
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing

2	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy
3	Switch should support the complete STACK of IPv4 and IPv6 services.
4	The Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied
5	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking
	Hardware and Interface Requirement
6	Switch should have the following interfaces:
	a. 48 x 1G/10G/25G Multi Mode Fiber Interface populated with 48*10G multi mode interfaces
	b. 6 x 40G /100G ports fully populated using multimode 100G SR Trancievers, for uplink connectivity
7	Switch should have console port
8	Switch should have management interface for Out of Band Management
9	Switch should be rack mountable and support side rails if required
10	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant
11	Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
12	Switch should have a minimum 40MB buffer of more.
13	Switch should have smart buffering mechanism to classify long lived versus short lived flows and must have capability to dynamically prioritize short lived flows during congestion to avoid packet drop of mission critical traffic.
14	Switch should support VLAN tagging (IEEE 802.1q)
15	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
16	Switch should support Configuration roll-back and check point
17	Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc
	Performance Requirement
18	Switch should support Graceful Restart for OSPF, BGP etc.
19	Switch should support minimum 512 VRF instances
20	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high-availability during primary controller failure
21	The switch should support hardware based loadbalancing at wire speed using LACP and multi chassis etherchannel/LAG
22	Switch should support minimum 3.6 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) including the services:
	a. Switching
	b. IP Routing (Static/Dynamic)
	c. IP Forwarding
	d. Policy Based Routing
	e. QoS
	f. ACL and Other IP Services

	g. IPv6 host and IPv6 routing
	Advance Features
23	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE
24	Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center
25	Switch should support OpenFlow/Open Day light/Open Stack controller
26	Switch should support VXLAN routing (single pass without any re-circulation)
27	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically.
	Layer2 Features
28	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)
29	Switch should support VLAN Trunking (802.1q) and should support 3900 VLAN
30	Switch should support basic Multicast IGMP v1, v2, v3
31	Switch should support minimum 64K no. of MAC addresses
32	Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
33	Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
34	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third party switch or server
35	Switch should support Jumbo Frames up to 9K Bytes on all available Ports
36	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
37	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
	Layer3 Features
38	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
39	Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
40	Switch should support MPLS segment routing and VRF route leaking functionality from day 1
41	Switch should provide mutlicast traffic reachable using:
	a. PIM-SM
	b. PIM-SSM
	c. IGMP v1, v2 and v3
	Availability
42	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy
43	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP
44	Switch should support for BFD For Fast Failure Detection as per RFC 5880
45	Quality of Service
46	Switch system should support 802.1P classification and marking of packet using:
	a. CoS (Class of Service)

	b. DSCP (Differentiated Services Code Point)
	c. Source physical interfaces
	d. Source/destination IP subnet
	e. Protocol types (IP/TCP/UDP)
	f. Source/destination TCP/UDP ports
47	Switch should support methods for identifying different types of traffic for better management and resilience
48	Switch should support for different type of QoS features for real time traffic differential treatment using
	a. Weighted Random Early Detection
	b. Strict Priority Queuing
49	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
50	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic
	Security
51	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
52	Switch should support control plane i.e. processor and memory protection from unnecessary or DoS traffic by control plane protection policy
53	Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4
54	Switch should support for external database for AAA using:
	a. TACACS+
	b. RADIUS
55	Switch should support DHCP Snooping
56	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol
57	Switch should support to prevent edge devices in the network not administrator's controlled from becoming Spanning Tree Protocol root nodes
58	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
59	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port
	Manageability
60	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
61	Switch should provide remote login for administration using:
	a. Telnet
	b. SSH v2
62	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
63	Switch should support for management and monitoring status using different type of Industry standard NMS using:

	a. SNMP v1 and v2
	b. SNMP v3 with encryption
	c. Filtration of SNMP using Access list
	d. SNMP MIB support for QoS
64	Switch should support for basic administrative tools like:
	a. Ping
	b. Traceroute
65	Switch should support central time server synchronization using Network Time Protocol NTP v4
66	Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces
67	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
68	Switch should provide different privilege for login in to the system for monitoring and management
69	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
	IPv6 features
70	Switch should support for IPv6 connectivity and routing required for network reachability using different routing protocols such
	a. OSPF v3
	b. BGP with IPv6
	c. IPv6 Policy based routing
	d. IPv6 Dual Stack etc
	e. IPv6 Static Route
	f. IPv6 Default route
	g. Should support route redistribution between these protocols
71	Switch should support multicast routing in IPv6 network using PIMv2 Sparse Mode
72	Switch should support for QoS in IPv6 network connectivity
73	Switch should support for monitoring and management using different versions of SNMP in IPv6 environment such as:
	a. SNMPv1, SNMPv2c, SNMPv3
	b. SNMP over IPv6 with encryption support for SNMP Version 3
74	Switch should support syslog for sending system log messages to centralized log server in IPv6 environment
75	Switch should support NTP to provide an accurate and consistent timestamp over IPv6 to synchronize log collection and events
76	Switch should support for IP V.6 different types of tools for administration and management such as:
	a. Ping
	b. Traceroute
	c. SSH
77	All relevant licenses for all the above features and scale should be quoted along with switch
78	Switch and optics should be from the same OEM
79	Comprehensive onsite hardware warranty for 3 years with Next business Day (NBD) resolution.

80	Online upgrade the version of firmware/software/patches as and when required.
	Software defined Storage For DR
SN	**Minimum specification required**
1	The solution should provide unified and centralized software defined platform that intergates market leading compute, storage, networking and security virtualization into a common platform to deliver enterprise-ready cloud infrastructure for the private and public cloud.
2	The solution should have capability to automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning.
3	The solution should provide a centralized Management and provisioning solution that understands the physical and logical topology of the provisioned data center and the underlying components
4	The solution should provide broad ecosystem to flexibly deploy on premises on certified hardware from major OEM vendors or run it as a service from AWS or from a selected number of Cloud Providers.
5	The proposed compute virtualization, software defined storage technology for HCI should be from vendors placed in the LEADERS quadrant in the latest respective Gartner Magic Quadrant reports available
6	The solution should be supportable by the vendor through a single point partner support organization for the software stack (compute, network, storage virtualization) and able to seamlessly integrate into an existing data center environment
7	The management components of the solution should have high availability that allows non-disruptive operation of the running workloads.
	Server Virtualization
8	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus, HIPS integration, replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, hot add of CPU, memory, devices for windows as well as linux VMs, VM level encryption, secure boot, vMotion within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology.
9	The server virtualizatoin managment solution should have the ability to expand up to at least 8 racks worth of servers without the need addition of additional management points
	Storage Virtualization
10	Should include storage virtualization /HCI software supporting all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any server manufacturer & should support mixing of different compatible Server brands in same Cluster. It should work on mutually certified hardware of any vendor like dell, HP, Cisco, Lenovo, Hitachi etc. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.
11	Storage virtualization should support VM-Centric controls for managing storage service levels for capacity, IOPS, availability QoS by storage policy-based management and should not be dependent on Luns. Should also support features like rack awareness, deduplication, compression & raid 5,6 through erasure coding (for all flash). Should also support scale up by adding disk in the node without any additional licenses, scale out by adding nodes.

12	The solution should provide storage systems for the software defined data center which pools together local flash devices and/or hard disks to provide a highly resilient shared datastore suitable for a variety of workload domains including business critical applications, virtual desktops, remote IT, DR, and DevOps infrastructure.
13	The solution should have an automated upgrade and patching process that allows full administrative control on the selection of storage software bundles, resources to upgrade and the timing of the upgrades and provide periodic pre-integrated and interop tested software bundles for patching and upgrade of the storage component products
14	The solution should have known industry standard hardware components with freedom of choice in terms of hardware between several hardware providers such as servers from major OEMs like Dell, Cisco, HP, Hitachi etc and and switches from Dell, Cisco, Arista etc.
15	The solution should have a simple way of adding incremental capacity in the form of servers or entire racks. This addition of capacity should NOT result in an increase of the number of management points
16	The solution should provide management of hardware system and the necessary functions required for discovering, bootstrapping, and monitoring the hardware, where it can access all hosts and switches on the out-of-band network.
17	The automated upgrade process should ensure that the running workloads are not affected by the upgrade and must provide protection through automated workload migrations as the upgrades happen.
	Network Virtualization
18	The network virtualization should provide distributed in-kernel routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN services, distributed L2-L4 stateful in kernel firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, vCenter objects and tags, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration)..
19	The solution should be capable to provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc
20	Solution provide traffic visibility (IPFIX), end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools.
21	The solution should have the ability to deliver end to end security for all applications by delivering network-level micro-segmentation, distributed firewalls, load balancers, virtual routers, virtual switches and VPN,
22	The solution should provide the network virtualization platform for software defined datacenter, delivering the operational model of a virtual machine for entire networks including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.
23	The solution should have highly granular (per VM or per VM interface) level security capabilities - potentially accessed through the network virtualization layer
24	The solution should support common L3 and L2 connectivity topologies to the existing datacenter network and choices on the amount of bandwidth that can be configured on its uplinks to the existing datacenter network. (Minimum of 80G)

25	The solution should have highly granular (per VM or per VM interface) level security capabilities - potentially accessed through the network virtualization layer
26	The solution should support heterogeneity from rack-to-rack if we choose to have different supported configurations by different vendors.
27	The solution should have high availability or redundancy built for its physical network.
28	The internal network should be built to be highly available with redundant links from servers to switches and link aggregation to provide aggregation and traffic load balancing
29	The solution should provide automated delivery of virtual networking & virtual security services such as switching, routing, load balancing and firewalling.
	Cloud Orchestration
30	Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS/ SaaS services so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM and movement within and across DC & DR.
31	The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific cloud and IT resources, while ensuring compliance with business policies
32	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows based on SOAP/REST operations and PowerShell scripts
33	The solution should have the ability to create custom workflows to automate the delivery of anything as a service - XaaS (for example Email, Storage as a Service, Network as a Service , Backup as a Service etc.)
34	The solution should provide for creation of complete application blueprints along with required virtual networking (routing, load balancing) and security services for the application using a user friendly graphical interface by using drag & drop functionality
35	The solution should have a Unified graphical canvas for designing machines, software components and application stacks with the ability to extend or define external integrations in the canvas through XaaS
36	The private cloud management solution should support for heterogenous virtualization platform. Vmware ESXi 6.5 or later, Microsoft Hyper-V, System Center 2016 or above, RedHat virtualization
37	The solution must provide visibility and show back for all the VM's that are not deployed through Cloud Portal. System must provide management actions like resize, snapshot, reboot, power on/off etc for existing VM's not deployed through the automation tool.
38	The solution should provide flexibility in deployment with having cloud-independent application profile coupled with its cloud-specific orchestrator that abstracts the application from the cloud, interprets the needs of the application, and translates these needs to cloud-specific services and APIs. The tool should eliminate the need of cloud specific scripting and cloud lock-in.
39	The solution should provide true multi tenancy, Each tenant needs to be able to create their own profiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines.
40	The solution should include unique lifecycle management services that automate day 0 to day 2 operations, from bring up to configuration, resources provisioning and patching/upgrades.
41	The solution should be Integra table with existing datacenter services such as DNS, NTP, Active Directory

42	The virtual domains/group/DC should be elastically expandable to larger capacities when needed. This expansion should be non-disruptive to existing workloads and should be destroyable when not needed and the resources consumed by them returned to the available resource pool.
43	There should be application specific virtual domains/group/DC that can construct the full backend infrastructure needed for the application.
44	The information on the resources in use by any virtual domain/group/DC needs to be available at any given time. This information should include both the physical and management resources associated with the virtual domain(s)
45	The solution should provide automatic private cloud metering and consumption analysis
	Cloud Operations & Management
46	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. This should be for heterogenous environment including Vmware ESXi, Hyper-V, RHEV
47	Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.
48	Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.
49	Solution capacity analytics should provide "What If" scenarios for physical, virtual (VMware, Hyper-v, RedHat KVM) & container environment and provide infrastructure and operations, log analytics to eliminate time-consuming problem resolution processes through automated root cause analysis
50	The solution shall preemptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times
51	The health of the various subcomponents should be monitored and reported within the solution
52	The solution should provide alert management on problem detection. Each notification should include a clear description of the problem and provides remediation actions needed to restore service, degradations or failures are aggregated and correlated to workload/ virtual domains to enable a clear view of the impact of any issue.
53	The solution should deliver a single interface for heterogeneous and highly scalable solution of both physical and virtual components with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting
54	The solution should have the ability to provide information on aggregate capacity of the system both physical and virtual at any given time
55	The solution should have monitoring, auditing and logging capabilities built-in as part of cloud operations capabilities built-in for cloud operations for both physical and logical infrastructure
56	The solution should have an easy way to carve its total capacity into smaller pools of capacity (Virtual Domain/group/DC). e.g. for specific workload types
57	The virtual domains/group/DC in the solution should be policy controlled to provide specific capacity, availability and performance as required by workloads

58	The solution should provide Workload Automation capabilities. that dynamically defines and controls the environment in the Optimal State in real time. This should Enforce data sovereignty & business continuity policies for each workload by having full stak visibility including application (Websphere, weblogic, jboss, tomcat etc.) & database transactions (SQL, Oracle etc.) aware
59	OEM should provide direct support 24x7x365 with unlimited incident support for severity 1 with L1, L2, L3 level (Telephonic/ Web/ Email) and 30mins or less response time including the unlimited upgrades and updates for a period of 3 years from the date of commissioning.
60	All the components including Compute virtualization, Network virtualization, storage virtualization, Cloud Orchestration & Automation, Operations Management & Network analytics should be provided
61	Qty of all the components including Compute virtualization, Network virtualization, storage virtualization, Cloud Orchestration & Automation, Operations Management & Network analytics should be based on the Server/CPU/Cores/VM considered in the bid.
62	Support/Subscription for Above Software Suite (Per CPU/Server/VM) for 3 years

Solution for DR:

SN	Minimum Requirement Description
1	The solution provides centralized automated disaster recovery, site migration and non-disruptive testing capabilities to the customers.
2	The solution should work in conjunction with various replication solutions including both the VM/ Hypervisor based replication and array based replication to automate the process of migrating, recovering, testing, re-protecting and failing-back virtual machine workloads.
3	The solution should act as the same site to serve as a protected site and recovery site when replication is occurring in both directions and protecting virtual machines at both sites.
4	The migration of protected inventory and services from one site to the other should be controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools to which they are allocated, and the networks they can access.
5	The solution should be able to Map virtual machines to appropriate resources on the failover site
6	The solution should provide option to customize the shutdown of low-priority virtual machines at the failover site to get more resources or proper utilization of resource and should provide option to recover multiple sites into a single shared recovery site.
7	The solution should offer multiple recovery plans that can be configured to migrate individual applications and entire sites providing finer control over what virtual machines are failed over and failed back. Support the extension of recovery plans with custom scripts, control access to recovery plans with role-based access control. This also enables flexible testing schedules.
8	The solution should be able to initiate recovery plan execution from virtualization manager with a single click and able to support automated boot of protected virtual machines with pre-specified boot sequence.

9	The solution should offer: o Application-agnostic protection eliminates the need for app-specific point solutions o Automated orchestration of site failover and failback with a single-click reduces recovery times o Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives o Centralized management of recovery plans from the virtualization manager console replacing the manual runbooks o Planned migration workflow enables disaster avoidance and data center mobility o Reduce the DR footprint through hyper-converged, software defined storageo VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage o Support for array-based replication offers choice and options for synchronous replication with zero data loss o Self-service, policy based provisioning via Storage Policy Based Protection Groups, Orchestration and Automation layer automates protection""
10	The solution should be able to manage and monitor execution of recovery plans from virtualization manager and support automated reconfiguration of virtual machine IP addresses at failover site. Should receive automatic alerts about possible site failure.
11	The solution should be able to automate failback to original production site using original recovery plan and also able to automatically re-protect virtual machines by reversing replication to the original site.
12	The solution should be able to use storage snapshot to perform recovery tests without losing replicated data and also provide multiple point-in-time recovery which will allow reversion to earlier known states.
13	The solution should enable the non-disruptive testing of recovery plans, using a temporary copy of the replicated data, and isolated network and storage environments in a way that does not disrupt ongoing operations at either site. This provides for the ability to test disaster recovery, disaster avoidance, or planned migrations as frequently as desired to ensure confidence in the configuration and operation of recovery plans.
14	The solution should be able to store, view and export results of test and failover execution from virtualization manager and automate cleanup of testing environments after completing tests.
15	It should be able to manage replication directly through virtualization manager, at a granular virtual-machine level. Ensure complete replication of virtual machine data in an application-consistent state, prior to initiating migration.
16	The solution should provide storage-agnostic replication that supports use of low-end storage, including direct-attached storage and also provides host based replication which will replicate only changed blocks to increase network efficiency.
17	The solution should provide automatic generation of history reports after the completion of workflows such as a recovery plan test and cleanup are performed in DR solution. These reports should document items such as the workflow name, execution times, successful operations, failures, and error messages which are useful for internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to HTML, XML, CSV, Microsoft Excel, Word document.
18	The solution should provide support for Stretched Storage, orchestrated cross site Virtual Machine migration and integration with Software defined network solutions
19	OEM should provide direct support for L1, L2 and L3 levels 24x7x365 with unlimited incident support and 30 mins or less response time including the unlimited upgrades and updates for a period of 3 years from the date of commissioning.
20	Qty of all the components including above Disaster Recovery License should be based on the Server/CPU/Cores considered in the bid.
21	Support/Subscription for Above Software Suite (Per CPU/ per Server/ per VM) for 3 years

****

CHAPTER-3-B

INSPECTION AND INSTALLATION, TESTING & COMMISSIONING

1. TESTS AND MEASUREMENTS

All equipment's shall be subjected to tests as per technical specification and requirement specified in Chapter-3, Part-A, at manufacturer facility/premises and a test report for each equipment duly signed by the testing authority and accepted by suitable authority shall be submitted along with the equipment.

1.1 TEST CATEGORIES

1.1.1 The following tests shall be conducted for acceptance of the equipment and the system before final acceptance of the system.

i) Factory Acceptance Testing (FAT)
ii) Pre-commissioning test (after installation) for total integrated system.
iii) Site Acceptance Testing (SAT)
i) Trial Run / Field Trials.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.1.2 These tests shall be carried out on all equipment supplied by tenderer including those supplied by sub-vendors, if any. Tenderer shall arrange all necessary test instruments, manpower, test-gear, accessories etc.

1.1.3 All technical personnel assigned by Tenderer shall be fully conversant with the system specifications and requirements. They shall have the specific capability to make the system operative quickly and efficiently and shall not interfere or be interfered by other concurrent testing, construction and commissioning activities in progress. They shall also have the capability to incorporate any minor modifications/suggestions put forward by Purchaser/Engineer.

1.1.4 Test Plan: The Contractor shall submit to Purchaser 'Test Plans' well in advance of commencement of actual testing in each of the above mentioned test categories.

The plans shall include:

1.1.4.1 System/Equipment functional and performance description (in short) and Tests to be conducted and purpose of test.

1.1.4.2 Test procedures (including time schedule for the tests) and identification of test inputs details and desired/expected test results

1.1.5 Test Report: The observations and test results obtained during various tests conducted shall be compiled and documented to produce Test Reports by Tenderer. The Test Reports shall be given for each equipment/item and system as a whole. The report shall contain the following information to a minimum:

1.1.5.1 Test results

1.1.5.2 Comparison of test results and anticipated/expected (as per specifications) test result as given in test plans and reasons for deviations, if any.

1.1.5.3 The data furnished shall prove convincingly that:

a. The system meets the Guaranteed Performance objectives
b. Mechanical and Electrical limits were not exceeded.
c. Failure profile of the equipment during the tests are well within the specified limits.

1.1.6 Failure of Cards/Components:

Till the system is accepted by the Purchaser, a log of each and every failure of cards/components shall be maintained. It shall give the date and time of failure, description of failed component/ card with serial no., lot no. etc, circuit, module, component designation, effect of failure of component on the system/ equipment, cause of failure, date and time of repair, mean time to repair etc. Repair/modification done at any point of time at one site shall be carried out by Tenderer at all the sites. Detailed documentation for the same shall be submitted to Purchaser for future reference.

If the malfunction and/or failures of a unit/module/sub-system/equipment repeat during the test, the test shall be terminated and Tenderer shall replace the necessary component or module to correct the deficiency. Thereafter, the tests shall commence all over again from the start.

If after the replacement the equipment still fails to meet the specification, Tenderer shall replace the equipment with a new one and tests shall begin all over again. If a unit/ subsystem/module have failed during the test, the test shall be suspended and restarted all over again only after the Tenderer has placed the Equipment back into acceptable operation. Purchaser's approval shall be obtained for any allowable logical time required to replace the failed component/unit/module/sub-system.

1.1.7 Re-adjustments

No adjustments shall be made to any equipment/cards during the acceptance tests. If satisfactory test results cannot be obtained unless readjustments are made, Tenderer shall carry out only those readjustment needed to ready the equipment/system for continuance of tests. A log of all such adjustments shall be kept giving date and time, equipment, module, circuit, adjustments, reasons, test result before and after adjustment etc. Fresh acceptance tests shall be conducted after the readjustments have been completed.

1.2 FACTORY ACCEPTANCE TESTING (FAT)

Factory acceptance tests shall be carried out after review and approval of FAT procedure/documents as per bid requirements and review of Pre-Factory acceptance results & shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are offered. The factory acceptance testing shall be conducted in the presence of the Purchaser/Engineer.The tests shall be carried out on all equipment/items including those supplied by Sub-vendors and factory acceptance certificates shall be issued. The factory tests shall include but not be limited to:

1.2.1 Equipment Testing:

1.2.1.1 Mechanical checks to the equipment for dimensions, inner and outer supports, finishing, welds, hinges, terminal boards, connectors, cables, painting etc.
1.2.1.2 Electrical checks including internal wiring, external connections to other equipment etc.
1.2.1.3 Check for assuring compliance with standards mentioned in the specifications.
1.2.1.4 Individual check on each/module/sub-assembly in accordance with the modes and diagnostics programs of the Tenderer
1.2.1.5 Checks on power consumption and heat dissipation characteristics of various equipment.
1.2.1.6 Environment testing and other laid down tests in Type Tests plan of the specification of the equipment.
1.2.1.7 Functional testing
1.2.1.8 Any other test not included in FAT document but relevant to the project as desired by the Purchaser/Engineer at the time of factory acceptance testing.

All equipment's materials fittings and components will be subject to inspection by the purchaser or his representative at the manufacturer's factory/tenderer works before dispatch and no materials shall be dispatched until these are inspected and/or approved.

Under exceptional circumstance, if it is not feasible to conduct Factory Acceptance Testing (FAT) at manufacturing facility, the equipment shall be accepted on the basis of certified manufacturer test report. In that case preliminary inspection of the equipment shall be arranged by the vendor at a suitable facility within India and detail inspection at site as per mutually agreed testing procedure. Exemption of inspection at factory premises (FAT) will be at the sole discretion of RailTel.

1.2.2 System Integration Testing

Functional and performance test should be conducted for the complete system/ all major equipment constituting the system (including the equipment supplied by sub-vendors, as applicable) simulating the complete network with appropriate network elements. All equipment shall be connected using the same cables (interfaces/components) as will be used during final installation so that the system can be tested in its final configuration. This testing shall be conducted at the manufacturing facility of the main equipment.

1.3 INSTALLATION:

After successful completion of Factory Acceptance Test or acceptance report of equipment on the basis of certified manufacturer test report, equipment shall be sent to site for installation.

All equipment shall be checked for completeness as per the specifications of equipment required for a particular station. Installation shall be carried out in accordance with the installation manuals and approved installation drawings in the best workmanship.

The contractor shall be responsible for ensuring that the work throughout are executed in the most substantial, proper and workmanlike manner with the quality of material and workmanship in strict accordance with the specifications and as per sound industrial practices and to the entire satisfaction of the RailTel.

If during installation and commissioning any repairs are undertaken, the maintenance spares supplied with equipment shall not be used for the repair. Tenderer shall arrange his own spare parts for such activities till such time the system has been finally accepted by the Purchaser. A detailed report & log of all such repairs shall be made available by the Tenderer to Purchaser/Engineer and shall include cause of faults and repair details, within two weeks of fault occurrence.

Tenderer shall supply all installation materials required for proper installation of the equipment. These shall include but not be limited to, all connectors, inter-bay and inter-equipment cables, power/earthing cables, connectors, anchoring bolts, nuts, screws, washers etc. as needed.

The bidder has to ensure that installation of equipment shall be done as to present neat and clean appearance in accordance with approved installation document drawings. All inter bay, power supply and other cables shall be routed through wall mounted cable trays. No cable shall be visible. Equipment installed at one of the site shall be made as model site and Tenderer shall take approval from Purchaser/engineer on various aspects etc.

1.4 PRE-COMMISSIONING

On completion of installation of equipment, the correctness and completeness of the installation as per Manufacturer's manual and approved installation documents shall be checked by the Tenderer on his own.

A list of Pre-Commissioning tests (same as approved by the Purchaser/Engineer for Site Acceptance Testing) and activities shall be prepared by Tenderer and the test shall be carried out by the Tenderer on his own. After the tests have been conducted to the Tenderer own satisfaction, the Tenderer shall provide the test results for review by Purchaser/Engineer and then offer the system for Site Acceptance Testing.

During pre-commissioning, if any fault occurs to any equipment or system, Tenderer shall identify the same and provide report/history of all faults to the Purchaser.

Tenderer shall ensure that the spares meant for operation and maintenance are not used during installation and commissioning.

1.5 SITE ACCEPTANCE TESTING (SAT)

On completion of Pre-commissioning, site acceptance testing shall be conducted on the system as per approved SAT procedures and its constituents by the Tenderer under the presence of Purchaser/Engineer.

The tests shall include, but not be limited to the following:

1.5.1 Checks for proper installation as per the approved installation drawings for each equipment/item and system as a whole.
1.5.2 Guaranteed performance specifications of individual equipment/item.
1.5.3 Self diagnostics test on individual equipment
1.5.4 Tests on metering and alarm panels
1.5.5 Tests on remote alarm transmission and reception
1.5.6 System tests on per hop basis and END TO END for the ring/link, all complete.

1.6 PROVISIONAL ACCEPTANCE CERTIFICATE (PAC)

On installation of the equipment, the contractor shall certify and advise Railtel Supervisor where equipment has been installed, in writing that the installation is (i) completed (ii) ready for satisfactory commercial service and (iii) ready to be handed over. After successful completion of Site Acceptance Testing, a report (SAT) shall be forwarded to ED/DNM. Provisional Acceptance Certificate (PAC) will be issued by ED/DNM. PAC will not be held back for want of minor deficiencies not affecting the functioning of the equipment. Deficiencies, if any, pointed at the time of issuance of PAC, will be rectified by the contractor within one month.

1.7 TRIAL RUN/FIELD TRIALS

Upon conclusion of the site acceptance testing, the Tenderer shall keep the facilities commissioned for one month for 'TRIAL RUN/FIELD TRIALS'. During this period Tenderer shall provide all specialist Engineers & Technicians including experts at the NMS to maintain the total log, incidents, failures & for assisting site engineer & for total co-ordination. However, the normal operation and maintenance of the system shall be performed by the personnel of the Purchaser trained for the purpose.

If during 'TRIAL RUN/FIELD TRIALS' any defect is noted in the system, the Tenderer shall rectify, replace the same to the satisfaction of Purchaser/Engineer. The decision to repeat the final test or restart the 'Trial / Field Trials' shall be of Purchaser/Engineer depending upon the severity of the defect.

During trial run / field trial, if any fault occurs to any equipment of system, Tenderer shall identity and rectify the same and provide report, history of all faults to the Purchaser.

Ideally, during the 'TRIAL RUN / FIELD TRIALS', no shutdown of the system due to failure of equipment, power supply etc. should happen. A record of all failures shall be kept for each manned/unmanned station and the availability of the system on per hop and end to End basis shall be calculated, accordingly and results submitted to Purchaser/engineer. If the system fails to come up to the guaranteed performance, the Tenderer, within a period of thirty (30) days shall take any and all corrective measures and resubmit the system for another 'Trial Run' of trial period. All modifications, changes, corrective measures, labour etc. shall be at the cost of the Tenderer. In case the date of completion for the second trial run exceeds the time schedule for the project, he shall be liable to pay liquidated damages. If the system fails to reach the guaranteed performance even after the second trial run, the Purchaser shall be free to take any action as he deems fit against the Tenderer and to bring the system to the guaranteed performance with the help of third party at the expense of the Tenderer.

1.8 FINAL ACCEPTANCE CERTIFICATE (FAC)

The final acceptance of the works completed shall take effect from the date of successful completion of 12 months after issue of PAC provided in any case that the contractor has complied fully with his obligations in respect of each item under the contract. The Final Acceptance Certificate of all regions against the contract shall be issued by ED/DNM. Notwithstanding the issue of Final Acceptance Certificate, the contractor and the purchaser shall remain liable for fulfillment of any obligation incurred under the provision of the contract prior to the issue of Final Acceptance Certificate which remains unperformed at the time such certificate is issued and for determining the nature and extent of such obligation the contract shall be deemed to remain in force between the parties hereto.

1.9 QUALITY ASSURANCE

1.9.1 Tenderer shall submit the details of Quality Assurance program followed by them beginning with raw materials, active, passive and fabricated components, units, sub-assemblies, assemblies, wiring, interconnections, structures etc. to finished product. Tenderer shall obtain and forward the Quality Assurance Program for equipment supplied by Sub-vendor, if any.

1.9.2 The Purchaser/engineer reserves the right to inspect and test each equipment at all stages of production and commissioning of the system. The inspection and testing shall include but not be limited to raw materials. Components, sub-assemblies, prototypes, production units, guaranteed performance specifications etc.

1.9.3 For inspection and testing, Tenderer shall arrange all that is required e.g. quality assurance personnel, space, test instruments etc. for successful carrying out of the testing by the Purchaser/Engineer, at Tenderer cost, at the Manufacturer's works/tenderer premises/site.

1.9.4 Purchaser/Engineer shall have free entry and access to any and all parts of the Manufacturer's facilities associated with manufacturing and testing of the system at any given time.

1.9.5 It shall be explicitly understood that under no circumstances shall any approval of the Purchaser/Engineer relieve the Tenderer of his responsibility for material, design, quality assurance and the guaranteed performance of the system and its constituents.

1.9.6 Tenderer shall invite the Purchaser/Engineer, at least 7 days in advance, of the date at which system shall be ready for Inspection and Testing. All relevant documents and manuals approved Engineering drawings etc. shall be available with the Purchaser/Engineer well in advance of the start of Inspection and Testing.

1.9.7 Purchaser or his representative shall, after completion of inspection and testing to their satisfaction, issue factory acceptance certificates to release the equipment for shipment. No equipment shall be shipped under any circumstances unless a factory acceptance certificate has been issued for it, unless agreed otherwise by Purchaser/Engineer.

****

CHAPTER-3-C

TRAINING, VENDOR DATA REQUIREMENT, DOCUMENTATION, AND DESIGN GUIDELINES

1. TRAINING

Tenderer shall train personnel of Purchaser/engineer in all aspects of offered system.

The training course shall be conducted at the manufacturing facilities from where the respective equipment/subsystems are manufactured/ offered or in India if the firm can arrange full fledged training facilities in case their manufacturing facilities are located outside India.

It shall be explicitly understood, that Purchaser's/Engineer's personnel shall be fully associated during Engineering, Installation, Testing and Commissioning activities and this opportunity shall be taken by Tenderer to impart on the job training in addition to the above training course.

Tenderer offer excludes costs of transportation, lodging and boarding of the trainees which shall be arranged by the Purchaser.

The training course to be conducted at the manufacturing facilities shall be designed to train the trainees in all aspects of System engineering, equipment operation, installation and functional details, theory of operation of equipment, trouble shooting and familiarization with the equipment at card and component level. All equipment used for training shall be identical to those quoted and supplied for site installation in hardware and software versions.

Tenderer shall provide comprehensive documentation, course material, manuals, literature etc. as required for proper training of personnel at his own cost. Consolidated and comprehensive documentation shall be available to each participant. After the completion of course, all such materials shall become the property of the PURCHASER. Tenderer shall update the course material of manuals in case there are any changes owing to revision/modifications in equipment/system specifications.

Tenderer shall, prior to start of training, send complete training program including details of each course, duration, subject matter etc. The Purchaser/Engineer reserves their right to suggest any additions/deletions in the program, which shall be incorporated by the Tenderer at no additional cost.

2. VENDOR DATA REQUIREMENT AND DOCUMENTATION

One set of Documentation shall be supplied with each system. In addition, 12 more sets of full documents shall be supplied. All documents and manuals shall be in English language only.

The following documents for the complete system shall be supplied and approved by Purchaser/Engineer in order to start inspection:

a. System description, System configuration diagram & Connectivity diagram
b. Detail technical manual of each type of equipment
c. Equipment interconnection diagram including details of various interfaces, signaling protocols used at each stage.
d. Layout of equipment and space requirements for each station.
e. Installation manual including installation procedure and commissioning.
f. Supervisory configuration, alarm list, operator interface etc.
g. Maintenance manual of each type of equipment containing:
    i. Preventive maintenance procedures.

ii. Trouble shooting/repairs procedures including failure analysis shall provide exhaustive information about repairs including but not limited to removal, reinsertion of components and cards, repairs, adjustments, tuning, calibration, tools required for a particular operation, test points, including turnaround time for repair and the details of the maintenance support service center to be furnished in the bid and all other maintenance related details.

iii. Expansion possibilities of the system without causing deterioration in the system performance.

iv. Any other data, document not specifically mentioned, but required for the satisfactory testing, installation and commissioning, operation and maintenance of the system shall be provided.

v. Documents to be supplied after trial runs but before System commissioning (Acceptance of the System by Purchaser/Engineer).

3. DESIGN GUIDELINES

i) Equipment shall conform to the similar housing standards and shall preferably be integrated in one 19"/21" rack.

ii) All equipment shall have sufficient number of alarms and supervisory indications and shall be provided with self-diagnostic facilities. All alarms and monitoring & diagnostic facilities shall be built-in & shall be displayed on the front panel of the equipment for ease of maintenance. It shall be possible to transmit these indications, parameters to the control station /NMS on real time basis.

iii) The healthy/unhealthy condition of the units shall be displayed by different color LEDs/Lamps.

iv) For important switches, the maintenance personnel shall provide controls on the front panel with suitable safeguard to avoid accidental operation. Manual changeover should be performed by more than one sequential operating procedure to avoid accidental operation.

v) All equipment shall be immune to EMI; RFI interference generated by any nearby source & shall meet the latest international standards in this regard.

vi) The equipment shall be capable of functioning with minimum maintenance and shall be preferred to have no requirement of any preventive maintenance.

vii) All patch cords shall be provided with connectors matching to the cable used and shall have identification markings.

viii) All sub-assemblies or modules, switches and controls and the circuit components shall be so mounted as to permit their replacement without appreciable disturbance to other components.

ix) If the vendor is not using distributed power supply system on individual module basis then the Power supply cards shall be duplicated (1+1). However one standalone power supply card shall be able to run the system for its entire lifetime.

x) All equipment sub racks, housings shall be provided with antistatic wristbands, if required for safe handling of Cards.

xi) The equipment should have modular design and should be configurable in number of operational modes to perform complex and different network functions without need of any additional software.

****

CHAPTER 4

COMMERCIAL TERMS & CONDITIONS

1. Offer letter and Validity of offer

1.1. The bidder shall complete the offer letter (Chapter 1) and the Price Schedule (Chapter 2)furnished in the tender documents, indicating the goods to be supplied, description of the goods, associated technical literature, quantity and prices etc.

1.2. The offer should remain valid for a minimum period from the date of opening of tender including the date of opening as indicated in Bid Data Sheet (BDS) Chapter 5.

2. Warranty

2.1. The warranty would be valid for a period as indicated in Bid Data Sheet (BDS) Chapter 5. The supplier shall warrant that stores to be supplied shall be new and free from all defects and faults in material, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards of materials of the type ordered and shall perform in full conformity with the specifications and drawings. The supplier shall be responsible for any defects that may develop under the conditions provided by the contract and under proper use, arising from faulty materials, design or workmanship such as corrosion, inadequate quantity of material to meet equipment requirements, inadequate contact protection, deficiencies in design and/ or otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser who shall state in writing in what respect the stores are faulty.

2.2. If it becomes necessary for the contractor to replace or renew any defective portion/portions of the supplies under this clause, the provisions of the clause shall apply to the portion/portions of the equipment so replaced or renewed or until the end of the above-mentioned period or twelve months, whichever may be later. If any defect is not remedied within a reasonable time of 30 days, the Purchaser may proceed to do the work at the contractor's cost, but without prejudice to any other rights which the Purchaser may have against the contractor in respect of such defects

2.3. Replacement under warranty clause shall be made by the contractor free of all charges at site including freight, insurance and other incidental charges.

2.4. Warranty Support

2.4.1. Material for repair during Warranty Period shall be handed over /taken over to contractors engineer at RailTel Data Center Gurgaon/Secunderabad or nearest RailTel PoP.

2.4.2. During the warranty period, the contractor shall be responsible to the extent expressed in this clause for any defects that may develop under the conditions provided for by the contract and under proper use, arising from faulty materials, design or workmanship in the plant, or from faulty execution of the plant by the contractor but not otherwise and shall remedy such defects at his own cost when called upon to do so by the Purchaser Engineer who shall state in writing in what respect the portion is faulty.

2.4.3. During the free warranty maintenance period contractor should stabilize the working of the system. Purchaser has the right to extend the period of supervision of the maintenance free of cost till the system stabilizes and works satisfactorily for a reasonable period of time. If during the time any equipment etc. is to be added or

deficiencies are to be rectified to make the system work trouble free the same also will have to be done by the contractor at no cost to RailTel as to make good all the deficiencies.

2.4.4. In case of hardware failure the replacement must be given in next business day If the Bidder fail to replace as per below mentioned duration, the following penalties will be imposed. It will be calculated on quarterly (3 month) basis and maximum penalties will be 10 % of the cost of Equipment per year.

2.4.5. Replacement Services

During warranty and AMC period, if the Bidder fails to replace /Equipment card/Part in next business day, the following penalties will be imposed.

Equipment	**Duration of repair**	**Deduction/Penalties**
All Modules and accessories	More than 1 days and up to 7 days	2% of the cost of affected part/module
All Modules and accessories	More than 7 days and up to 15 days	10% of the cost of affected part/module
All Modules and accessories	More than 16 days and up to 30 days	25% of the cost of affected part/module
All Modules and accessories	More than 30 days	100% of the cost of affected part/module

Note:

a. In event of that bidder fails on both service SLA and replacement services the maximum aggregate penalties would be limited to equipment cost.

b. OEM should provide facility to RailTel for direct fault case open on TAC Support in case emergency.

2.5. Maintenance Supervision

2.5.1. After the proposed network is commissioned and placed in service and after Provisional Acceptance Certificate (PAC) is issued, the contractor shall be responsible for proper maintenance supervision of the network free of cost for a period of twelve months from the Successful commissioning of the solution.

2.5.2. To summarize, the total period of warranty as per BDS in Chapter-5, will comprise of first 12 months of Maintenance Supervision (after issue of PAC) extendable by RailTel for reasons as explained, as per para 2.5 above, posts which FAC will stand issued.

3. **Long Term Maintenance Support**

3.1 Tenderer (OEM) shall provide maintenance support after successful completion of the warranty obligations for a minimum period of 5years. The long term maintenance support shall be comprehensive and include all hardware and software of equipment supplied against this contract. RailTel should be extended the benefits of periodical software patches/updates made by OEM on the system from time to time for equipment security/performance without any additional cost to RailTel.

3.2 Tenderer/OEM(through its Indian subsidiary), shall be paid @ 3.5% of supply cost per annum towards Long Term Maintenance Support after completion of warranty period, to undertake repairs/replacements of all type of module/ card/assembly/ subassembly and update/upgrade of software released during this period and /or which may fail in the network after the warranty. Only incremental cost in % over and above this, if perceived

by the OEM and Tenderer, may be indicated in Schedule of Requirement and shall be added to the equipment cost towards evaluation of tender. If however the tenderer feels that his AMC Cost is less than 3.5% per annum, he should give suitable discount in equipment pricing. For AMC he will be paid @ 3.5% per annum only. If the Tenderer quotes a higher base rate for AMC, he will be paid at his quoted rate per annum and five years differential cost shall be added to offered cost for evaluation. AMC would have to be valid for minimum period of 5 years after the warranty.

In case tenderer quotes AMC rates lower than 3.5%, no advantage will be given to him for evaluation purposes. In case the tenderer wins the contract his cost will be reduced by differential (w.r.t. 3.5%) AMC rates & he will be paid accordingly. AMC charges to him, however be paid only @ 3.5% per annum.

3.3 Separate agreement for AMC (Long term Maintenance Support) before expiry of warranty period shall be entered with OEM/the authorized partner of OEM by RailTel. A fresh Bank Guarantee @10% of issued LOA/PO value valid for 64 months (4 months beyond the AMC period of 5 years)from the date of issue of LOA shall be required to be submitted by OEM/ Tenderer for due fulfillment of long term maintenance support obligation.

3.4 Quarterly payment for AMC Charges would be made by RailTel after successful completion of AMC Services of that quarter and on the certificate furnished by concerned RailTel representative of the CNOC.

Note: The acceptance of the above clause is mandatory and specific acceptance from OEM is required to be enclosed as per Form no.3. Any deviation / non acceptance will lead to rejection of the bid summarily

4. Delivery Period

The materials as per SOR are required to be delivered within period as indicated in Bid Data Sheet (BDS, Chapter 5) to the site /transported to different locations which will be provided by RailTel to the successful bidder.

5. Payment Terms

5.1 Payment shall be made in Indian Currency (Rs) 75% payment of the value of the supply items would be made on receipt of material by the consignee(at site / the stores) duly inspected and on submission of the following documents subject to any deductions or recovery which RailTel may be entitled to make under the contract:

- Invoice (GST)
- Delivery Challan/e-way bill.
- Packing list.
- Factory Test Report/Certified manufacturer Test Report
- Purchaser's Inspection certificate
- Consignee receipt
- Warranty certificate of OEM
- Insurance certificate
- Certificates duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.

5.2 15% payment of the value of Supply items of the PO shall be made by RailTel on successfully Installation & Commissioning at site, 5% payment of value of Supply items of the PO on issue of Provisional Acceptance Certificate (PAC) and the last 5% payment of the value of Supply items of the PO shall be made by RailTel on issue of Final Acceptance Certificate (FAC) which will be issued by ED/DNM.

5.3 15% payment of value of supply items of the PO which could not be installed within 90 days due to site readiness or other reason on account of RailTel will be made with approval of ED/DNM and remaining (5% + 5%) on issue of PAC and FAC.

5.4 RailTel shall make payments after the submission of invoice with required documents as per contract.Accounting/Bill passing unit for SOR for supplies is Corporate Office. All Bills shall be submitted to the ED/DNM for certifying and verification and onwards submission to Finance of RailTel Corporate Office for releasing the payment.

5.5 Deleted.

5.6 The breakup of taxes has to be furnished and same should be reflected in the bills so that any CENVAT/input credit can be availed by RailTel.

5.7 Payment of Services Items

5.7.1 Payment of service items shall be made in Indian Currency (INR) only. 90% payment of SOR item towards “Installation, Testing & Commissioning" shall be made by Corporate Office on successful Installation, testing & commissioning, 5% on issue of PAC and final 5% on issue of Final Acceptance Certificate.

5.7.2 Payments for Resident Engineer will be paid on quarterly basis after satisfactory go ahead from competent authority.

5.7.3 Payment of SOR item towards “AMC" would be paid quarterly by the Corporate Office after satisfactory completion of AMC Services of that quarter and on certificate furnished by DC Team.

6. Performance Bank Guarantee (Security Deposit)

6.1 The successful bidder has to furnish security deposit in the form of Performance Bank guarantee @ 10% of issued PO/ LOA value, the same should be submitted within 30 days of issue of LOA/PO, failing which a penal interest of 15% per annum shall be charged for the delay period i.e. beyond 30 (thirty) days from the date of issue of LOA/PO. This PBG should be from a Scheduled Bank and should cover warranty period plus three months for lodging the claim. The performance Bank Guarantee will be discharged by the Purchaser after completion of the supplier's performance obligations including any warranty obligations under the contract.

6.2 The earnest money shall be released on submission of PBG. The Performa for PBG is given in Chapter 6 Form No. 1. If the delivery period gets extended, the PBG should also be extended appropriately.

6.3 The Performance Bank Guarantee (security deposit) will bear no interest.

6.4 This PBG would be released after satisfactory completion of contract including warranty period and only after submission of 10 % PBG towards AMC.

6.5 A separate advice of the BG will invariably be sent by the BG issuing bank to the RailTel’s Bank through SFMS and only after this the BG will become acceptable to RailTel. It is therefore in interest of bidder to obtain RailTel’s Bank IFSC code, Its branch and address and advise these particulars to the BG Issuing bank and request them to send advice of BG through SFMS to the RailTel’s Bank.

7. Taxes & Duties

7.1 The price quoted in the offer should be firm, fixed indicating the break up and inclusive of all taxes and duties like import, custom, anti-dumping, CGST, IGST, SGST, UTGST etc. The offer should be inclusive of packing, forwarding, freight up to destination, insurance charges.

7.2 Bidder shall issue valid tax invoice to RailTel for availing proper credit of CGST/SGST/IGST/UTGST in case of award of contract. GST will not be reimbursed in the absence of valid tax invoice.

7.3 For all the taxable supplies made by the vendor, the vendor shall furnish all the details of such taxable supplies in the relevant returns to be filled under GST act.

7.4 If the vendor fails to comply with any of the above, the vendor shall pay to purchaser any expense, interest, penalty as applicable under the GST act.

7.5 In case of incorrect reporting of the supply made by the vendor in the relevant return, leading to disallowance of input credit to purchaser, the vendor shall be liable to pay applicable interest under the GST act to the credit of purchaser. The same provisions shall be applicable in case of debit/credit notes.

7.6 Tenderer shall quote all-inclusive rates, but there shall be break up of basic price and all type of applicable taxes such as SGST/CGST/IGST/UTGST along with respective HSN/SAC code under GST law(Including tax under reverse charges payable by the recipient).

7.7 Wherever the law makes it statutory for the purchaser do deduct any amount towards GST at sources, the same will be deducted and remitted to the concerned authority.

7.8 The imposition of any new tax and/or increase/ in the aforesaid taxes, duties, levies, after the last stipulated date for the receipt of tender including extensions if any and the bidder there upon necessarily and properly pays such taxes/levies/cess, the bidder shall be reimbursed the amount so paid, provided such payments, if any, is not, in the opinion of RailTel attributable to delay in execution of work within the control of bidder. The bidder shall within a period of 30 days of the imposition of any such tax or levy or cess, give a written notice thereof to RailTel that the same is given pursuant to this condition, together with all necessary information including details of input credit relating thereto. In the event of no payment/default payment of any of the above taxes, RailTel reserves the right to withhold the dues/payments of bidder and make payment to states/central government authorities as may be applicable. However, if the rates are reduced after the last stipulated date for receipt of tender, bidder has to pass on the benefits to RailTel.

7.9 In case of imported equipment:
Anti-Dumping duty if applicable on the equipment proposed to be supplied by OEM/Tenderer as per extant instructions of Ministry of Commerce/Finance Government of India, has to be borne by the tenderer and shall be deducted from the amount payable to the bidder at the time of making payment to the firm, if this duty amount is paid to custom Authority by RailTel.

7.10 Inter se position of the offers will be determined on total unit rate on CIP destination basis which will include basic rate, custom duty, CGST, SGST, IGST, UTGST, freight, Insurance and any other charges or cost quoted by the tenderer, including GST payable on reverse charge by RailTel, whenever applicable.

7.11 In regards to works contract, the tenderer should have registration no. for GST in respective state where work is to be executed and shall furnish GST registration certificate on award of LOA.

8. Insurance

8.1 The Contractor shall take out and keep in force a policy or policies of insurance from the date, the delivery of material starts (including the transit portion) against all liabilities of the Contractor or the Purchaser. The contractor shall take out and keep in force a Policy or policies of Insurance for all materials covered in schedule of requirement irrespective of whether used up in the portion of work already done or kept for the use in the balance portion of the work until such material are provisionally handed over to RailTel. The goods will be issued by purchaser to supplier and risk of goods shall remain with supplier until the issue of PAC by RailTel. Insurance policy has to be kept valid by the contractor till issue of PAC by RailTel.

8.2 The Contractor should insure the stores brought to site, against risks as required under the Emergency Risk (Goods) Insurance Act in force from time to time up to contract value.

8.3 It may be noted that the beneficiary of the insurance policy should be RailTel or the policies should be pledged in favor of RailTel. The contractor shall keep the policy/policies current till the equipment are handed over to the purchaser. It may also be noted that in the event of contractor's failure to keep the policy current and alive, renewal of policy will be done by purchaser for which the cost of the premium plus 20% of premium shall be recovered from the contractor.

9. Liquidated Damages

The timely delivery is the essence of this tender. Liquidated damages will be applicable at the rate of half percent per week or part thereof for undelivered portion of SOR subject to a maximum of 10% of the cost of Purchase order for any reason whatsoever attributed to failure of tenderer. RailTel will have the right to cancel the order, place order on alternative source besides levying the liquidated damages as above.

10. Transportation

The rates quoted should be CIP destination. The destination sites will be provided by RailTel to the successful bidder.

11. Statutory Deduction

These will be made at source as per the rules prevalent in the area of work.

12. Qualification Criteria

Qualifying criteria under this clause lays down minimum acceptable qualifications in various areas to ensure that qualified tenderer has necessary experience, technical expertise, equipment and financial and human resources to successfully complete the project. Bids from bidder not meeting these qualification criteria shall be summarily rejected.

12.1 Technical Capability

12.1.1 The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender (as indicated in Bid Data Sheet (BDS) Chapter 5). The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test

equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied.

12.1.2 The Tenderer/bidder should have supplied and provision of similar offered equipment's of security solution commercially with satisfactory working as indicated in Bid Data Sheet (BDS) Chapter 5 to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.

12.1.3 The Bidder should have registered office in India for a minimum period of 3 years as on originally scheduled date of bid opening.

12.1.4 The Bidder should have authorization from respective OEMs and should submit the vetted BOM from their respective OEMs.

12.1.5 Each OEM can authorize up to a maximum of three (3) authorized partners to bid the tender.

12.1.6 The Bidder or their promoters having equity stake or operating partnership in bidder, should not be holding valid License for Telecom service provider/ISP/NLD, Services License of Government of India for Telecom Operation.

12.1.7 RailTel reserves the right: -

a) To verify, if so desired, the correctness of documentary evidence furnished by the tenderer.
b) To verify the successful operation and performance of qualifying projects and tenderer shall arrange permission for the same.
c) To carry out capability assessment of the bidder(s) including referral to in-house information.
d) RailTel shall not be responsible for any delay in the receipt of tenders and reserves the right to accept/reject any or all tenders without assigning any reason.

12.1.8 The bidder shall furnish documentary proof of backend support including software upgrades and availability of spares for a period of 5 years from the respective OEMs of the products offered.

12.1.9 The tenderer/OEM should submit the details of supply of offered equipment executed as indicated in Bid Data Sheet (BDS) Chapter 5, along with certificates from the original user for whom the project was undertaken certifying the date of award of contract, date of completion, and the present working state of the system which should clearly bring out performance of the equipment. The certificates are to be submitted in original or their true copies duly signed by the tenderer.

12.2 Financial Criteria

12.2.1 The bidder should be a company registered under the Companies Act, 1956/2013 or a partnership firm registered under Indian Partnership Act 1932 or Limited Liability Partnership Act 2008 with registered office in India and in operation for at least 3 years from the date of opening of tender and should have their registered offices in India.

Valid documentary proof of:

- Certificate of Incorporation
- Certificate of Commencement of Business.
- Certificate consequent to change of name, if applicable
- Copy of Memorandum of Association.

12.2.2 The company must be registered with appropriate authorities for all applicable statutoryduties/taxes.

12.2.3 Valid documentary proof of:
- a) Income Tax registration/PAN number
- b) GSTIN Number

12.2.4 Income Tax returns for the last three years.

12.2.5 The tenderer should present at least one (1) project worth as indicated in Bid Data Sheet (BDS) Chapter 5showcasing supply, installation,testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years.

Copy of work orders supported with relevant documentary evidences for the same and the completion certificates by the client.Documentary evidence should clearly indicate the nature of systems implemented for each project

12.2.6 The sum total of the turnover (i.e. revenue from operations) during the last preceding 3 financial years (i.e. current year and three previous financial years) from the date of opening of tender should be a minimum of the value as indicated in Bid Data Sheet (BDS) Chapter 5.

12.2.7 Tenderer should produce Audited Balance Sheet and Income statement of all the preceding three financial years.

12.2.8 The tenderer shall furnish such documents as to establish the financial soundness of their company. The latest balance sheet audited or certified by a neutral agency shall be furnished.

12.2.9 In the event of foreign Original Equipment Manufacturer (OEM), Indian Subsidiary is allowed to participate with the experience and financial credential of parent company with specific authorization for doing so from the OEM. The specific authorization addressed to RailTel should be submitted by the tenderer.

13. System Performance Guarantee

13.1 The tenderer shall give unqualified and unconditional guarantee that when the equipment / material supplied by him is installed and commissioned at site, it shall achieve the desired objective and that in the event of performance of the system when installed not complying with the end objective or with the specifications, he shall provide further inputs to enable the RailTel to realize the end objectives with full compliance of the specifications contained in these documents. No additional payment will be made to the contractor for supply of any additional goods and service required in this regard.

13.2 This certificate in the Proforma given in Chapter 6 Form No. 2, shall accompany the final offer. Absence of this certificate which will form part of the agreement shall disqualify the tenderer automatically.

14. Evaluation of Offer

14.1 For the purpose of relative ranking of offers, all-inclusive value for entire supply, supervision of installation, testing & commissioning and warranty period support, training, AMC shall be taken into account.

14.2 Additional features offered by the bidder, over and above the ones asked for in the tender documents, shall not be considered for evaluation of bids.

14.3 The tenderer should make available the offered products, if desired during technical evaluation of offered equipment for testing and benchmarking at any testing facility approved by RailTel.

14.4 The bidders should quote for all items & the offer will be evaluated in totality. The bidders should indicate brand name, type/model number of the products offered. Optional items will be considered for evaluation of offers. The equipment should be supplied as per Technical Specifications given in Chapter-3.

15. Security Considerations & Security Agreement

15.1 While evaluating the tender, regards would be paid to National Defence and Security considerations.

15.2 The directives issued from time to time by the Department of Telecommunications (DoT), Ministry of Communications and IT or any other Ministry of Govt. of India on security considerations shall be applicable to the present tender. Accordingly, as per the extent amendment of the National Long Distance (NLD) Service License Agreement for Security related concerns for expansion of Telecom Services in various zones of the country issued vide Department of Telecommunication, Ministry of Communication and IT, Govt. of India's letter no. 10-54/2010-CS-III (NLD) dated: 31.05.2011, the successful tenderer/OEM shall comply with the provisions stated in the above mentioned directive of DoT and shall have to enter into an agreement with RailTel as per the template agreement between Telecom Service Provider and the vendor of equipment, product and services (available on DoT website). The tenderer must submit a declaration along with their bid.

15.3 The Network is being provided primarily to meet the requirement of Indian Railways. Accordingly, the network shall take into consideration the National Security requirement and National Security aspects indicated by the Indian Railways.

16. Purchaser's Right to Vary Quantities

The purchaser shall be at liberty to enhance or reduce the quantity mentioned in the purchase order as indicated in Bid Data Sheet (BDS) Chapter 5 without assigning any reasons. The bidder shall comply with such modifications unconditionally provided these are made before completion of the deliveries under the purchase order. Any such change in quantity shall have no impact on the rates mentioned in the purchase order for any such item.

17. Purchaser's Right to accept any offer / Bid and to reject any or all offer/ Bid

The Purchaser reserves the right to accept or reject any offer / bid, and to annul the bidding process and reject all offers / bids, at any time prior to award of order without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds for the Purchaser's action.

18. Execution of Purchase Order

18.1 The successful bidder has to submit the copy of the Purchase order duly signed on each page including Annexures & will submit the Performance Bank Guarantee as per Clause no. 6 for due fulfillment of the PO.

18.2 If the successful bidder fails to submit the accepted copy of PO and required PBG within 30 days from the date of issue, it shall constitute a breach of the agreement affected by the acceptance of the tender in which case the full value of the earnest money accompanying the tender shall stand forfeited without prejudice to any other rights or remedies. The Tenderer shall also submit the inspection plan, Implementation plan etc, within 30 days period.

18.3 In the event of any tenderer, whose tender is accepted, refuses to execute the PO as herein before provided, RailTel may determine that such tenderer has abandoned the Purchase Order and thereupon his tender and acceptance thereof shall be treated as cancelled and RailTel shall be entitled to forfeit the full amount of the Earnest Money and to recover the damages for such default.

19. Annulment of Award

Failure of the successful bidder to comply with the requirement of various clauses of tender document shall constitute sufficient ground for the annulment of the award and forfeiture of EMD in which event the Purchaser may make the award to any other bidder at the discretion of the Purchaser or call for new offers/ bids.

20. Earnest Money Deposit (EMD)/ Bid Security

20.1 The tenderer shall furnish a sum as given in Bid Data Sheet (BDS) Chapter 5 as Earnest Money through IREPS Portal.]

20.2 The EMD may be forfeited if a bidder withdraws his offer or modifies the terms and conditions of the offer during validity period and in the case of a successful bidder, if the bidder fails to accept the Purchase order and fails to furnish performance bank guarantee (security deposit) in accordance with clause 6.

20.3 Offers not accompanied with Earnest Money shall be summarily rejected.

20.4 Earnest Money of the unsuccessful bidder will be discharged / returned as promptly as possible but not later than 30 days after the expiry of the period of offer / bid validity prescribed by the Purchaser.

20.5 The successful bidder's EMD will be discharged upon the bidder's acceptance of the purchase order satisfactorily and furnishing the performance bank guarantee in accordance with clause 6.

20.6 Earnest Money will bear no interest.

21. Preference to make in India

Preference to make in India will be applicable as per (i) Ministry of Commerce and Industry / Department of Industrial Policy and Promotion (Public procurement Section) notification No. P-45021/2/2017-PP (BE-II) dt. 28.05.2018 and (ii) Ministry of Communication/ Department of telecommunications notification number 18-10/2017-IP dt. 29.08.2018 or any latest notification issued by Government of India.

22. Offer/ Bid Prices

22.1 The bidder shall give the prices indicating all levies and taxes, packing forwarding, freight and insurance etc. The basic unit price and all other components of the price need to be individually indicated against the goods it proposes to supply under the tender document

as per schedule given in Chapter 2. The price shall be quoted in Indian Rupees or in any major foreign currency for the imported items (FOR/CIP destination).

22.2 The breakup of price of each item of SOR in terms of basic Unit price, Excise duty, Sales Tax, Freight, Custom Duty, Forwarding, Packing, Insurance and any other Levies/charges already paid or payable by the tenderer shall be quoted in the SOR Chapter 2. Any changes in statutory duties/taxes after opening of technical bid will be to RailTel's account within the contracted delivery period.

22.3 All prices and other information like discounts etc. having a bearing on the price shall be written both in figures and in words in the prescribed offer form (SOR). In case of difference in words and figures, the amount written in words will be taken into consideration. In the event of any discrepancy between total unit cost and total cost, the value shown in total unit cost will be taken for evaluation purpose.

22.4 Fall Clause: - The tenderer shall undertake that in case the tenderer offers same type of material at a lower price to any other purchaser including Central/State/ Government Organization or Public Sector Undertaking, during the validity of purchase order, the equal benefit of lower prices will be passed on to RailTel. The tenderer will submit an undertaking to this effect while claiming the payment.

23. Clause wise Compliance

Clause wise compliance statement of the Technical Specifications (Chapter 3) and Commercial Terms & Conditions (Chapter 4) shall be enclosed with the offer along with the technical literature of the material and other documents in support of relevant clauses.

24. Inspection

24.1 Pre-shipment / pre-dispatch inspection shall be carried out at manufacturer's / tenderer's works/site by RailTel's authorized representative. At least part of the material should be offered for inspection within 60 days of issue of confirmed Purchase Order. Traveling, lodging & boarding expenses of RailTel's representative and charges for 3rd party inspection if any shall be borne by RailTel but necessary facilities to carry out tests/witness inspection shall be provided by the manufacturer/ tenderer, free of cost. Under exceptional circumstance, if it is not possible to carry out pre-dispatch inspection at manufacturer's premises, Exemption for the same shall be obtained from competent authority.

24.2 Along with inspection call, the tenderer/manufacturer shall submit details of test procedures, test programme, test parameters together with permitted values, etc. and their Quality Assurance Plan.

24.3 In case material fails during inspection, the fresh lot of material shall be offered without any extra cost, by the manufacturer/tenderer. In such a case, total cost of re-inspection including travel, lodging & boarding of the inspecting officials shall be to manufacturer's/ tenderer's account.

25. Force Majeure

25.1 If during the Agreement, the performance in whole or in part, by either party, of any obligation under this is prevented or delayed, by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD (hereinafter referred to as

EVENTS), provided notice of happenings of any such EVENT is given by the affected party to the other, within twenty one (21) days from date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non-performance or delay in performance. Provided service under this Agreement shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

25.2 In the event of a Force Majeure, the affected party will be excused from performance during the existence of the Force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this Agreement. Neither party shall be liable for any breach, claims, damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

26. Settlement of Disputes

26.1 Any dispute or difference whatsoever arising between the parties out of or relating to the construction, meaning, scope, operation or effect of this contract or the validity or the breach thereof shall be settled by arbitration in accordance with the Arbitration and Conciliation Act, 1996 as amended and the award made in pursuance thereof shall be binding on the parties. The venue of such arbitration or proceedings thereof shall be New Delhi.

26.2 All arbitration proceedings shall be conducted in English. Recourse against any Arbitral award so rendered may be entered into court having jurisdiction or application may be made to such court for the order of enforcement as the case may be.

26.3 The Arbitral Tribunal shall consist of the sole Arbitrator appointed by mutual agreement of the parties.

26.4 Each of the parties agree that notwithstanding that the matter may be referred to Arbitrator as provided herein, the parties shall nevertheless pending the resolution of the controversy or disagreement continue to fulfill their obligation under this Agreement so far as they are reasonably able to do so.

27. Governing Laws

The Purchase Order shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

28. Termination for Default

The purchaser may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Tenderer, terminate this contract in whole or in part.

28.1 If the tenderer fails to deliver any or all of the goods within the time period(s) specified in the contract.

28.2 If the tenderer fails to perform any other obligation(s) under the contract; and

28.3 If the tenderer, in either of the above circumstance(s) does not remedy his failure within a period of 30 days (or such longer period as the Purchaser may authorize in writing) after receipt of the default notice from the Purchaser.

28.4 In case of any of the above circumstances the RailTel shall pay the supplier for all products and services delivered till point of termination as per terms and conditions of the contract. However, any recovery and losses occurred to RailTel will be recovered from Contractor up to the value of contract.

29. Risk & Cost

If the contractor fails to deliver the equipment or honor the contractual commitment within the period fixed for such delivery in the contract, the Purchaser may terminate the Purchase contract in whole or in part, the Purchaser may proceed to purchase, upon such terms and in such manner as it deems appropriate, goods similar to those undelivered at no risk and cost to contractor. However, the security deposit of tenderer shall be forfeited/ Performance Bank Guarantee shall be encashed. The failed tenderer shall not be permitted to take part in the tender for balance work.

30. Termination for Insolvency

The purchaser may at any time terminate the Purchase order by giving written notice to the tenderer, without compensation to the tenderer, if the tenderer becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Purchaser.

31. Rates during Negotiation

The tenderer/s shall not increase his/their quoted rates including payment terms in case the RailTel Administration negotiates for reduction of rates. Such negotiations shall not amount to cancellation or withdrawal of the original offer and the rates originally quoted will be binding on the tenderer/s.

32. Clarification Requests

It is solicited that the written queries/ clarifications may be sent to the RailTel's office latest by date as indicated in the Bid Data sheet (BDS) through e-mail to rajeevkumar@railtelindia.comwith copy to asablania@railtelindia.com (in word format) & hard copy by post. All relevant clarifications sought will be addressed during the pre-bid meeting scheduled as per BDS.

33. Submission of Offers

33.1 All offers in the prescribed forms should be submitted before the time and date fixed for the receipt of the offers.

33.2 In case the schedule of requirement quoted by tenderer is incomplete with reference to tender document, the offer is liable to be rejected.

33.3 ATTESTATIONOFALTERATION: No scribblingis permissible in the tender documents. Tender containing erasures and alterations in the tender documents are liable to be rejected. Any correction made by the tenderer/ tenderers in his/their entries must be signed (not initialed) by him/them.

33.4 The tenderer shall submit his tender in sealed cover on specified date & time as mentioned in BDS Chapter 5. Each copy of the tender shall be complete in all respects. The copies should be marked "tender name & no". The original tender paper purchased from this office or down loaded from the RailTel web site shall be returned duly signed on each page along with the original offer.

33.5 The offer shall be submitted in two packet. Both Bids Credential Bid (Techno-Commercial Bid) &Price Bidshall be sealed in separate envelopes and both envelopes put in one large envelope. Both envelopes should bear the Tender No., its description and date of closing/opening. The bid shall consist of following documents:-

33.5.1 Offer Letter complete.
33.5.2 Schedule of Requirements with quantities but with prices blanked out (this will be a replica of price bid with prices blanked out).
33.5.3 Earnest Money in prescribed form.
33.5.4 Audited balance sheet duly attested by Notary Public.
33.5.5 Constitution of Firm and Power of Attorney.
33.5.6 Clause wise compliance to tender conditions.
33.5.7 Copies of purchase orders and other documents in support of meeting qualifying criteria.
33.5.8 Complete technical data and particulars of the equipment offered, as specified in the Tender papers together with descriptive literature, leaflets, Drawings, if any, complete with list etc.
33.5.9 Documentary proof of equipment being proven and working for more than 6 months in India or outside India along with user certificate and Contact Details of user/firm.
33.5.10 Technical proposal of tenderer in conformity with system design or alternative proposal of the tenderer, if any.
33.5.11 System Performance Guarantee as per Chapter 6 Form no. 2
33.5.12 The manufacturer claiming to qualify under the scope of rules for PMA(Preferential Market Access) must submit the declaration of VA (Value Addition) as required under the issued notification for the specified period (2015-16,2016-17& 2017-18).
33.5.13 Any other information desired to be submitted by the tenderer.
33.5.14 NIL Deviation certificate.

34. Constitution of Firm and power of Attorney

34.1 Any individual(s) signing the tender or other documents connected therewith should specify whether he is signing:-

34.1.1 As sole proprietor of the concern or as attorney of the sole Proprietor.
34.1.2 As a partner or partners of the firm.
34.1.3 As a Director, Manager or Secretary in the case of Limited Company duly authorized by a resolution passed by the Board of Directorsor in pursuance of the authority conferred by Memorandum of Association.

34.2 In the case of a firm not registered under the Indian Partnership Act, all the partners or the attorney duly authorized by all of them should sign the tender and all other connected documents. The original Power of Attorney or other documents empowering the individual or individuals to sign should be furnished to the Purchaser for verification, if required.

34.3 The RailTel will not be bound by Power of Attorney granted by the tenderer or by the changes in the composition of the firm made subsequent to the execution of the contract agreement.

34.4 In case where the Power of Attorney partnership deed has not been executed in English, the true and authenticated copies of the translation of the same by Advocate, authorized translators of Courts and Licensed Petition Writers should be supplied by the Contractor(s) while tendering for the work.

34.5 The duly notorised Power of Attorney shall be submitted in original or duly signed.

35. Opening of Bids:

35.1 Bids received form the Bidders shall be opened on due date and time. The opening of the Bids shall be carried out in the physical presence of the designated representatives of RailTel and the Bidders. However, this RFP does not mandate the physical presence of the Bidders. The absence of the physical presence of the Bidders shall in no way affect the outcome of the evaluation of the Bids. During bid opening, only two authorized representatives of each bidder shall be allowed to be present.

35.2 RailTel shall subsequently examine and evaluate the Bids in accordance with the provisions set out in this Chapter.

35.3 To facilitate evaluation of Bids, RailTel may, at its sole discretion, seek clarifications in writing from any Bidder regarding its Bid.

36. Non-Transferability & Non-Refund ability

The tender documents are not transferable. The cost of tender paper is not refundable.

37. Errors, Omissions & Discrepancies

The Contractor(s) shall not take any advantage of any mis-interpretation of the conditions due to typing or any other error and if in doubt, shall bring it to the notice of the purchaser without delay. In case of any contradiction only the printed rules, and books should be followed and no claim for the mis-interpretation shall be entertained.

38. Wrong Information by Tenderer

If the tenderer/s deliberately gives/give wrong information in his/their tender which creates/create circumstances for the acceptance of his/their tender the RailTel reserves the right to reject such tender at any stage.

39. The envelope shall be addressed to the Purchaser at the following address:

Executive Director/DNM
RailTel Corporation of India Ltd.
Plot No. 143, Institutional Area,
Opposite-Gold Souk,
Sector-44, Gurgaon-122003

Note: The envelope shall bear name of the tender, the tender no. and the words "DO NOT OPEN BEFORE" (due date).

40. Offer / Bid should be delivered to the above address so as to reach up to 15:00 Hrs of due date. The offers / bids shall be opened at 15:30 Hrs on the same day in the above office in the presence of those representatives of the bidders who choose to be present. Offers / Bids received after due date and time shall be dealt as per extant rules.

In case the date of opening happens to be a holiday, the tender will be received and opened at the same time on the next working day.

41. Limitation of Liability

Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law:

41.1 The Supplier shall not be liable to the Purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Purchaser; and

41.2 The aggregate liability of the Supplier to the Purchaser, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Purchaser with respect to intellectual property rights infringement.

42. Credential Verification

42.1 The tenderer shall submit along with the tender document, documents in support of his/their claim to fulfill the eligibility criteria as mentioned in the tender document. Each page of the copy of documents/ certificates in support of credentials, submitted by the tenderer, shall be self-attested/digitally signed by the tenderer or authorized representative of the tendering firm. Self-attestation shall include signature, stamp and date (on each page). Only those documents which are declared explicitly by the tenderer as "documents supporting the claim of qualifying the laid down eligibility criteria", will be considered for evaluating his/their tender.

42.2 The tenderer shall submit a notarized affidavit on a non-judicial stamp paper stating that they are not liable to the disqualified and all their statements/documents submitted alongwith bid are true and factual. Standard format of the affidavit to be submitted by the bidder is available in Chapter-6 of this tender document (Form No. 4). Non-submission of an affidavit by the bidder shall result in summary rejection of his/their bid and it shall be mandatory incumbents upon the tenderer to identify, state and submit the supporting documents duly self-attested by which they/he is qualifying the Qualification Criteria mentioned in the tender document. It will not be obligatory on the part of the RailTel to scrutinize beyond the submitted document of tenderer as far as his qualification for the tender is concerned.

a. The RailTel reserves the right to verify all statements, information and documents submitted by the bidder in his tender offer, and the bidder shall, when so required by the RailTel, make available all such information, evidence and documents as may be necessary for such verification. Any such verification or lack of such verification, by the RailTel shall not relieve the bidder of its obligations or liabilities here under nor will it affect any rights of the RailTel thereunder.

b. In case of any wrong information submitted by the tenderer, the contract shall be terminated, Earnest Money Deposit (EMD), Performance Guarantee (PG) and Security Deposit (SD) of contract forfeited and agency barred for doing business on entire RailTel for 5 (five) years.

43. Mandatory updation of Labour Data on Railway's shramikkalyan portal:

43.1 Contractor is to abide by the provisions of Payment of Wages Act & Minimum Wages act in terms of clause 54 and 55 of Indian Railways General Condition of Contract. In order to ensure the same, an application has been developed and hosted on website 'www.shramikkalyam.indianrailways.gov.in'. Contractor shall register his firm/company etc. and upload requisite details of labour and their payment in this portal. These details

shall be available in public domain. The Registration/updation of Portal shall be done as under:

(a) Contractor shall apply for onetime registration of his company/firm etc. in the Shramikkalyam portal with requisite details subsequent to issue of Letter of Acceptance. Engineer shall approve the contractor's registration on the portal within 7 days of receipt of such request.

(b) Contractor once approved by any Engineer, can create password with login ID (PAN No.) for subsequent use of portal for all LoAs issued in his favour.

(c) The contractor once registered on the portal, shall provide details of his Letter of Acceptance (LoA)/Contract Agreements on shramikkalyan portal within 15 days of issue of any LoA for approval of concerned engineer. Engineer shall update (if required) and approve the details of LoA filled by contractor within 7 days of receipt of such request.

(d) After approval of LoA by Engineer, contractor shall fill the salient details of contract labours engaged in the contract and ensure updating of each wage payment to them on shramikkalyam portal on monthly basis.

(e) It shall be mandatory upon the contractor to ensure correct and prompt uploading of all salient of engaged contractual labour & payments made thereof after each wage period.

43.2 While processing payment of any 'On Account bill' or 'Final bill' or release of 'Advances' or Performance Guarantee/Security deposit', contractor shall submit a certificate to the Engineer or Engineer's representatives that "I have uploaded the correct details of contract labours engaged in connection with this contract and payments made to them during the wage period in Railway's Shramikkalyam portal at 'shramikkalyam.indianrailways.gov.in ' till_____Month_____Year."

44. Integrity Pact Program:

a) RailTel has adopted Integrity Pact Program and for implementation thereof all tenders relating to procurement of OFC, quad cable, pre-fab shelters, electronic equipments and its installation and/or commissioning etc and other item(s) or activity/activities proposed to be carried out or required by the Company for the value exceeding Rs. 15 crores at a time including for repair and maintenance of cable/network and any other items required for special works assigned to RailTel will be covered under the Integrity Pact Program and the vendors are required to sign the IP document and submit the same to RailTel before or along with the bids.

b) Only those vendors who have purchased the tender document and signed the IP document can send their grievances, if any, to the Independent External Monitors (IEMNs) through the nodal officer.

Name of IEMs and contact details:

a) Sh. Ashok Kumar Garg, New Delhi e-mail: akgarg1654@gmail.com
b) Sh. Jayanta Kumar Roy, Kolkata e-mail: jkroy.its@gmail.com

c) If the order, with total value equal to or more than the threshold value, is split to more than one vendor and even if the value of PO placed on any/each vendor(s) is less than the threshold value, IP document having been signed by the vendors at bid stage itself, the Pact shall continue to be applicable.

d) Bidder of Indian origin shall submit the Integrity Pact (in 2 copies) on a non-judicial stamp paper of Rs. 100/- duly signed by the person signing the bid. If the bidder is a partnership or a consortium, the Integrity Pact shall be signed by all the partners or consortium members.

e) Bidder of foreign origin may submit the Integrity Pact on its company's letterhead, duly signed by the person signing the bid.

f) The 'Integrity Pact' shall be submitted by the Bidder duly signed in all pages along with the Bid in a separate envelope, duly superscripted with 'Integrity Pact'. Tender received without signed copy of the Integrity Pact document will be liable to be rejected. Proforma for signing the Integrity Pact is available in Chapter-6 of this tender document (Form No. 5).

g) One copy of the Integrity Pact shall be retained by RailTel and the 2nd copy will be issued to the representative of the bidders during bid opening. If the Bidders representative is not present during the Bid opening, the 2nd copy shall be sent to the bidder by post/courier.

****

CHAPTER-5

BID DATA SHEET (BDS)

The section consists of provisions that are specific to various Clauses of the tender document COMMERCIAL TERMS & CONDITIONS Chapter 4.

Clause	Description
Clause1.2	Validity of offer 60days.
Clause2	Warranty 36 months from the Date of System Commissioning (PAC) or 40 months from the date of delivery (Only in case the delay in system commissioning is on the part of consignee) whichever is earlier.
Clause 4	Delivery Period Delivery and supervision of installation and commissioning within 120 days of issue of LOA/PO.
Clause 12.1.1	**Technical Capability** The Tenderer/bidder should be an Original Equipment Manufacturer (OEM) or Authorized partner of OEM specifically authorized by OEM for bidding in this tender. The OEM should have proven facilities for Engineering, manufacture, assembly, integration and testing of offered system and basic facilities with respect to space, Engineering, Personnel, Test equipment, Manufacture, Training, Logistic Supports for at least past three years in the country from where the proposed equipment are planned to be supplied.
Clause 12.1.2	The Tenderer/bidder should have supplied and provision of similar offered security solutionwith satisfactory working as to Government/PSUs/Telecom Service Providers/Public Listed Company during the last three years from the date of opening of tender.
Clause 12.2.1	**Financial Criteria** i) The tenderer should present at least one (1) project worth at least INR 7.52Crore showcasing supply, installation, testing, commissioning, implementation and operations projects for Data Center solutions commercially in India in the last 3 years. Copy of work orders supported with relevant documentary evidences for the design parameters as mentioned in criteria 4 and the completion certificates by the client. Documentary evidence should clearly indicate the nature of systems implemented for each project ii) The sum total of the turnover (i.e. revenue from operations)during the last preceding 3 financial years from the date of opening of tender should be Minimum of Rs. 32.22Cr.

Clause	Description
Clause 16	Purchaser's Right to Vary Quantities Up to a maximum extent of +/- 30% ofSORquantity.
Clause 20	Earnest Money Deposit (EMD)/ Bid Security Rs. **12,24,000**/- (Rs. TwelveLakhTwenty FourThousand only)
Clause 32	Clarification Requests Last date of Submission of Clarification Date: 14.06.2019 (No query received after mentioned date will be entertained)
Clause 32	Pre Bid Meeting Deleted.
Clause 33	Last Date of Submission of Offer Date: 28.06.2019 Time: 15:00 hours Venue: same as above
Clause 35	Date of Opening of Tender Date: 28.06.2019 Time: 15:30 hours Venue: same as above

****

CHAPTER-6
Form No. 1
PROFORMA FOR PERFORMANCE BANK GUARANTEE BOND
(On Stamp Paper of Rs one hundred)

(To be used by approved Scheduled Banks)

1. In consideration of the RailTel Corporation of India Limited, having its registered office at 6th Floor, IIIrd Block, Delhi Technology Park,Shastri Park,Delhi-110053 (Herein after called RailTel) having agreed to exempt ……(Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Purchase Order No……dated……made between……and…….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs. ……(Rs …….. only). We …… (indicate the name of the Bank) hereinafter referred to as "the Bank") at the request of ……. ……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……. against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

2. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs . ……

3. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Tenderer(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Tenderer(s) shall have no claim against us for making such payment.

4. We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. …… We shall be discharged from all liability under this Guarantee thereafter.

5. We,…… (indicate the name of Bank) further agree with the RailTel that the RailTel shall have the fullest liberty without our consent

and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) / Tenderer(s).

(indicate the name of Bank) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

Dated the day of 2019

for ……..
(indicate the name of the Bank)
Witness

1. Signature
   Name

2. Signature
   Name

Form No. 2
PROFORMA FOR THE SYSTEM PERFORMANCE GUARANTEE
(On Stamp Paper of Rs.One hundred)

The Director,
RailTel Corporation of India Limited

I / We ……. hereby guarantee that the design on the basis of which we have submitted our tender no. …… has been carefully made to conform to the end objectives in the tender documents and to technical specification therein. We further guarantee that in the event of the performance of the system, when installed, not complying with the end objectives or with the specifications contained in the tender documents, we shall provide further inputs to enable the RailTel to realize the end objectives contained in these documents without any additional payment for any additional equipment which may be required in this regard. We further guarantee that all the expenses for providing the additional inputs under the System Guarantee will be borne by us. We further guarantee that these additional inputs will be provided by us to make the system workable within 1 month from the date on which this guarantee is invoked by the Purchaser. The guarantee is valid for a period of one year from the date of commissioning of the system.

(Signature of Firm's Authorized Officer)

Seal

Signature of witness:

1. …….

2. …….

Form No. 3

PROFORMA FOR THE LONG TERM MAINTENANCE SUPPORT
(To be signed by the O.E.M.)

To

The Director,
RailTel Corporation of India Limited

I / We ……. hereby confirm and accept that against RailTel Tender No. …….. , there is a requirement of Long Term Maintenance Support as per Clause 3. We confirm that Long Term Maintenance Support shall be met by us directly or through Authorized partner, as the case may be based on contracts. I / We have gone through the requirement mentioned in the Tender document and shall provide services for the offered supply items.

(Signature of Firm's Authorized Officer)
Seal

Signature of witness:

1. ……

2. …….

Form No. 4

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY TENDERER ALONGWITH THE TENDER DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 100/-. The paper has to be in the name of the tenderer) **

I……. (Name and designation)** appointed as the attorney/authorized signatory of the tenderer (including its constituents),

M/s _____(hereinafter called the tenderer) for the purpose of the Tender documents for the work of _____ as per the tender No. _____ of (RailTel Corporation of India Ltd.), do hereby solemnly affirm and state on the behalf of the tenderer including its constituents as under:

1. I/we the tenderer (s), am/are signing this document after carefully reading the contents.

2. I/we the tenderer(s) also accept all the conditions of the tender and have signed all the pages in confirmation thereof.

3. I/we hereby declare that I/we have downloaded the tender documents from RailTel/TCIL website www.railtelindia.com/www.tcil-india-electronictender.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the tender document. In case of any discrepancy noticed at any stage i.e. evaluation of tenders, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.

4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.

5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.

6. I/we declare that the information and documents submitted along with the tender by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.

7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of tenders, it shall lead to forfeiture of the tender EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the tenderer)** _____ and all my/our constituents understand that my/our constituents understand that my/our offer shall be summarily rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other

action provided in the contract including banning of business for five years on entire RailTel.

DEPONENT
SEAL AND SIGNATURE
OF THE TENDERER

VERIFICATION

I/We above named tender do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

SEAL AND SIGNAURE
OF THE TENDERER

Place:
Dated:

**The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by tenderer. Attestation before Magistrate/Notary Public.

Form No.-5

PROFORMA FOR SIGNING THE INTEGRITY PACT

RailTel Corporation of India Limited, hereinafter referred to as "The Principal".

And

……., hereinafter referred to as "The Bidder/ Contractor"

Preamble

The Principal intends to award, under laid down organizational procedures, contract/s for ……The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/transparency in its relations with its Bidder(s) and /or Contractor(s).

In order to achieve these goals, the Principal will appoint an Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1. The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

    a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

    b. The Principal will during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the process or the contract execution.

    c. The Principal will exclude from the process all known prejudiced persons.

2. If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2- Commitments of the Bidder(s) / Contractor(s)

1. The Bidder(s)/Contractor(s) commit 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(s)/contractor(s) will not, directly or through any other persons or firm, offer promise or give to any of the Principal'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 any advantage during tender process or during the execution of the contract.

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

c. The Bidder(s)/Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s) /Contractors will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the bidder(s)/contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractor(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers' as annexed and marked as Annexure A.

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

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

Section 3: Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings". Copy of the "Guidelines on Banning of business dealings" is annexed and marked as Annex-"B".

Section 4: Compensation for Damages

1. If the Principal has disqualified the Bidder(s) from the tender process prior to the awardaccording to Section 3, the Principal is entitled to demand and recover the damagesequivalent to Earnest Money Deposit/Bid Security.

2. If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to be terminated the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5: Previous Transgression

1. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti corruption approach or with any other public sector enterprise in India 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 for action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6: Equal treatment of all Bidders / Contractors/Subcontractors.

1. The Bidder(s)/Contractor(s) undertake(s) to demand from all subcontractors a commitment in conformity with this Integrity Pact, and to submit it to the Principal before contract signing.

2. The Principal will enter into agreements with identical conditions as this one with all bidders, contractors and subcontractors.

3. The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7: Criminal charges against violation by Bidder(s) / Contractor(s) / Sub contractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8: Independent External Monitor / Monitors

1. The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CMD, RailTel.

3. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Principal including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor(s)/Subcontractor(s) with confidentiality.

4. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

5. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

6. The Monitor will submit a written report to the CMD, RailTel within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

7. Monitor shall be entitled to compensation on the same terms as being extended to provided to Independent Directors on the RailTel Board.

8. If the Monitor has reported to the CMD, RailTel, a substantiated suspicion of an offence under relevant IPC/PC Act, and the CMD, RailTel has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9. The word 'Monitor' would include both singular and plural.

Section 9: Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 10 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded.

If any claim is made / lodged by either party during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of RailTel.

Section 10: Other Provisions

1. This agreement is subject to Indian Law, Place of performance and jurisdiction is the Registered Office of the Principal, i.e. New Delhi.

2. Changes and supplements as well as termination notices need to be made in writing.

3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

(For & on behalf of the Principal)
(Office Seal)

(For & On behalf of Bidder/Contractor)
(Office Seal)

Place ——————————

Date ——————————

Witness 1:
(Name & Address)

_____

_____

Witness 2:
(Name & Address)

_____

_____

END of Tender Document

****