Dated:03.07.2019

RailTel Corporation of India Ltd
(A Government of India Enterprise)

Plot No 143, Sector 44, Institutional Area,
Opposite to Gold Souk Mall,
Gurgaon, Haryana- 122003
Work: 0124-4236083
Fax: 0124-4236084

Website: www.railtelindia.com

Corrigendum-II

Sub: Request for proposals for "**Supply, Installation, Testing &Commissioning of Security Solution and Expansion of Cloud Infrastructure for Data Center (DC & DR) of RailTel.**"

Ref: i) This office Tender No. RAILTEL/TENDER/OT/CO/DNM/2019-20/DC Security & Cloud Infra/489 dated 06.06.2019.

In reference to the above referred tender the following amendment are issued under the Corrigendum-II. The bids may be submitted in consideration of this amendment.

1. Chapter-2, SCHEDULE OF REQUIREMENT may be read as:

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	No.	04				
SOR-B	Backup Solution as per Technical Specification given in Chapter-3A	No.	01				
SOR-C	UTM &Virtual Firewall as per Technical Specification given in Chapter-3A						
i)	Virtual Firewall Instance –L3	No.	03				
ii)	UTM	No.	02				
iii)	Firewall Manager (For virtual Firewall instances +UTM)	No.	01				
SOR-D	Security Detection and Analytics per Technical Specification given in Chapter-3A						
i)	Commercial SOC includes software components SIEM	No.	01				
ii)	Anti-Virus +EDR (Client)	Lot	01				
iii)	Anti-Virus + EDR (Server)	Lot	01				
iv)	Vulnerability Assessment Software Solution	No.	01				

v)	Application Black Box Scanner	No.	01				
vi)	Packet Capture	No.	01				
SOR-E	Cloud Solution in RailTel Data Center as per Technical Specification given in Chapter-3A						
i)	Rack Server	No.	24				
ii)	10G Switch as	No.	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.	No.	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)							

2. Chapter-2, Annexure-A, Tax Breakup for SOR may be read as:

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-D-v											
SOR-D-vi											
SOR-E-i											
SOR-E-ii											
SOR-E-iii											

3. Chapter-2, Foot Note No. VII may be read as:

The Bidder should have authorization specific to this tender from respective OEM.

3/7/19

4. **Chapter-3A, Point No.2 of Technical Requirement (The bidder has to carry out following activities) may be read as:**

   Bidder should have backend tie-ups with the respective OEMs to provide required technical support along with OEM or OEM nominated professional services partner 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.

5. **Chapter-3A, Added New Notes in Technical Requirement (The bidder has to carry out following activities):**

   Note 5: All the hardware offered against the tender should have redundant power supply.

   Note 6: It is bidders/OEM responsibility to provide Next Business Day (NBD) support for all the hardware supplied against the tender.

6. **Chapter-3A, Added New following points in Technical Requirement (The bidder has to carry out following activities from point no 04 to point no. 09):**

4 DC and DR overview:

Datacenter SOW –Statement of Work (or "SOW") that sets forth the roles and responsibilities of the Parties for the Data Center Services provided under the Agreement as part of the Services. These Services are the services and activities, as further detailed in this SOW, required to support Railtel DC at Gurgaon and DR at Secunderabad, all of the supporting infrastructure and security required to deliver the required Services and meet Service Level Requirements (SLRs).

Bidder Services environment includes centralized Unix-based, AIX- based, Linux-based, and Windows-based systems, associated with SDS and backup services, supporting systems Software (e.g., operating systems, utilities, databases, middleware, VMware) and Need to create DC with proper security by using major infra security products like WAF ,SIEM ,End points, HIPS etc.

5 Data Center Service Requirements:

Bidder shall be responsible for the following Data Center Services.

- 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.
- 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.

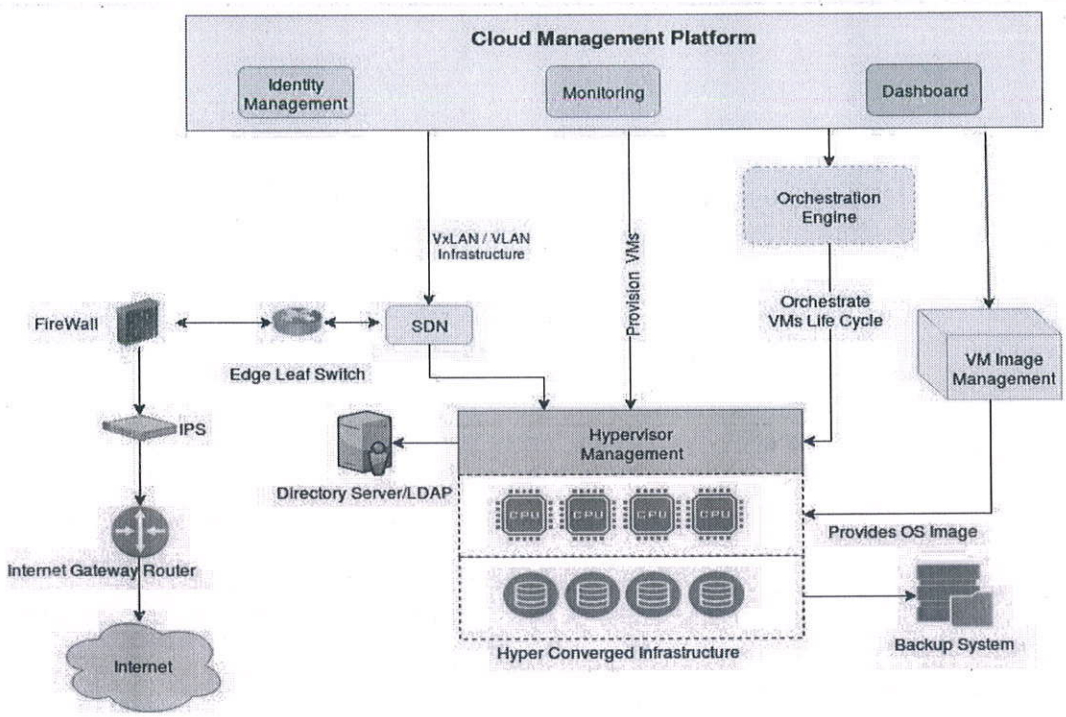
6 Scope of Work:

6.1 HCI based Railtel Cloud Deployment Architecture

3/7/19

HCI based RailTel Cloud will broadly comprise of Hyper Converged Infrastructure (HCI), Software defined Network (SDN) and Cloud Management platform (CMP) with backup solution.

Logical Architecture of HCI based RAILTEL Cloud



Scope of work for HCI Environment:

i. The bidder shall supply Hardware, Software, Network equipment and Network & Security software as per Schedule of Requirements and in accordance with minimum technical specifications as provided. Higher version /additional specifications shall be accepted. However, deviation from minimum specifications if any, shall be clearly indicated along with the explanation in the technical deviation section

ii. All the supplied equipment, licenses and ATS certificates should be in the name of RAILTEL.

iii. The bidder shall be responsible for providing all equipment, software and services, specified.

iv. For cloud management infra includes CMP, Virtualization Manager, SDN, SDS, NFV, Backup etc.

v. Bidders shall have back to back tie-up with OEMs (Minimum 60 Man-Days including all OEMs) of supplied product so as to provide support and professional services from the respective OEMs for deployment architecture, installation, configuration, performance tuning, security, acceptance testing and commissioning of the supplied products like Virtualization, CMP, HCI, SDN, Directory Service, Backup Solution, Switching infrastructure (Spine & Leaf), Virtual Firewall & Virtual Load Balancer, implementation of functional requirements and carry out required integration of various components offered in overall solution of HCI based RailTel Cloud..

vi. The bidder along with the OEM/s will work out and finalise the Deployment Architecture of the HCI based RailTel Cloud solution in coordination with customer with no single point of failure and in line with the industry best practices. Integration between various components offered in the overall solution needs to be done as indicated in the proposed deployment

3/7/19

architecture in section 4. The bidder shall arrange OEM/s resources of all supplied products at RAILTEL for finalization of the deployment architecture.

vii. Engineers from OEMs of all supplied products shall attend the pre-implementation meeting with RAILTEL for understanding of existing setup, discussing the technical requirements, deployment architecture and implementation plan and advising on deployment architecture including security features available in the supplied products that can be utilized in HCI based RailTel Cloud for improving the reliability, high availability, performance & security of the setup.

viii. Bidder shall configure Network Time Protocol (NTP) and Domain name Service (DNS) for HCI based RailTel Cloud.

6.2 Bidder shall perform following work for Network & Security equipment installation implementation & integration with existing Infrastructure:

i. Bidder shall provision the necessary Structured LAN cabling components for physical network connectivity of the new infrastructure as well as integration of HCI based RailTel Cloud with existing RAILTEL gateway. The bidder shall prepare a detailed plan to perform these activities. Planned downtime of appropriate duration shall be allocated for these activities during off peak hours.

ii. Respective OEMs of Firewall, Switches, Packet tracer, SDN Controller, Virtual Firewalls and Virtual Server Load Balancers shall also provide technical support for integration with Cloud Management Platform (CMP) being procured in this Tender. Bidder shall integrate Spine & Leaf Switches, SDN Controller, Virtual Firewalls and Virtual Server Load Balancers with CMP.

iii. Bidder along with OEM shall implement bi-directional integration of HCI based Cloud system with existing components installed in RAILTEL, Gurgaon.

iv. These components include Network & Security monitoring/management tools namely SIEM (Security Information and Event Management), VA (Vulnerability Assessment), and NMS (Network Management System).

6.3 Bidder shall perform following work for Hyper-Converged Infrastructure and Virtualization Software (Hypervisor) & Manager:

i. HCI solution should be delivered pre-configured (Software Defined Storage and Virtualization Software) and pre-tuned to reduce onsite deployment time.

ii. Create Virtualization environment as per the industry best practices in discussion with RAILTEL.

iii. Configure single centralized manager to control and manage the virtual infrastructure as well as for real time monitoring of both physical and virtual components.

iv. Configure Virtualization Management solution in distributed (with HA) model with no single point of failure.

v. Integrate Virtualization Manager with Cloud Management Platform (CMP), Software Defined Network (SDN) & Software Defined Storage (SDS).

vi. Configure network bonding, VLANs/VxLANs, tunnel wherever required and connectivity of all nodes with TOR switches (Leaf switches)

vii. Create Virtual machines for Linux OS or Windows, Virtual machine templates, Virtual machine configured in High Availability mode in cluster, affinity group creation of virtual machines and

virtual machine backup configuration (Snapshot and Clone).

viii. Configure storage policies to automate provisioning and balancing of storage resources to ensure that each VM gets the specified storage resources and services.

ix. Bidder shall perform integration of HCI with the supplied backup solution and should enable integration with VM to perform backup of VM data and configuration files e & backup appliance.

6.4 Bidder shall perform following work related to **System Security & Directory Services:**

i. Bidder shall implement and configure Directory Services as part of Overall solution so that all authentication, authorization of cloud Infrastructure is done by Directory Services.

ii. Bidder along with OEMs of Offered components will ensure that all the exposed APIs are designed, developed and tested as per OWASP Top 10 guidelines.

iii. Offered Solution of HCI based RailTel Cloud should not require downtime resulting in interruption of service or performance issues during application of Security Patches at any layer.

iv. Bidder shall be responsible for the base Images of OS are hardened as per RAILTEL Info-Sec Policy. The same will be shared by RAILTEL team at the time of pre-implementation meeting. The bidder will ensure that the security & resource monitoring agents for SIEM and NMS are preinstalled with base images.

v. Bidder shall also ensure that all other components like network devices, virtualisation layer etc. and all services offered under IaaS and PaaS are hardened as per RAILTEL Info-Sec Policy. Hardening guidelines shall be shared by RAILTEL team at the time of implementation.

6.5 Bidder shall perform following work related to **Cloud Management Platform (CMP): -**

i. bidder should integrate the CMP fully with the supplied HCI solution i.e., integration with manager of the hypervisor, Software Defined Network, Software Defined Storage, etc.

ii. The bidder should create self-service portal for automation and provision/ de-provisioning of data-centre services such as compute, storage, network, load balancing, backup, security and firewall.

iii. The bidder should integrate CMP with the supplied Directory Services software and should create business group as per the requirements given by the RAILTEL.

iv. The bidder should create policy-based controls of cloud resources and should configure Role-based policy management, administration and enforce role- based policies.

v. The bidder should create workflow and blueprints for IaaS, PaaS as defined in Functional Requirements

vi. The bidder shall also create basic & necessary reports for the analysis of resources (CPU, Memory, Storage and Network) utilization and available resources.

vii. The bidder should configure CMP to collect all the logs from the hypervisor layer, SDN layer & SDS layer for analysis and reporting. The bidder shall also create basic & necessary reports for the analysis.

viii. Bidder should configure auto-scaling of resource as per demand.

ix. The bidder should configure metering and show-back capabilities of CMP through appropriate

3/7/17

metrics in discussion with RAILTEL

x. The bidder should configure CMP with backup appliance, backup software & tape library to enable configuration of backup and restore through self- service Dashboard.

xi. The bidder shall configure REST base APIs with full API-level access to all functional components of the compute service such that any function available through the user interface is available through a REST API.

6.6 Bidder shall perform following work related to **Backup solution**:

i. Installation, Configuration, Testing and Commissioning of Purpose-Built Backup Appliance based Backup Solution at RAILTEL

ii. Integration with HCI Solution: Complete integration with the HCI solution including enabling of VM level integration and should have client-direct backup at the appliance through LAN. The integration should enable VM backup including its configuration and content also.

iii. Bidder should configure full, differential, incremental backup and restore of Configuration Management Databases of CMP

iv. Integration with CMP: complete integration to provide self- service configuration of data backup & restore facility

v. The Backup Solution furnished shall be complete in every respect with all required components and standard accessories normally provided with such equipment and/or needed for erection, completion and safe operation of the equipment as mentioned in technical specifications though they may not have been specifically detailed in the specification

UAT for HCI Environment:

i. Testing connectivity for HCI nodes, SDN and backup solution.

ii. Sizing of vm done as per customer requirement

iii. Verifying the vswitch creation as per needs

iv. Checking the policy and alerts in orchestra

v. Test recovery of one VM from backup solution

vi. Check the High availability, DRS is configured in Cloud management platform.

vii. Knowledge transfer to customer

viii. Configuration document submission to customer

7 Security solution Integration in Data centre -SOW:

7.1 SSL visibility Appliance

i. Bidder need to design logical and physical topology as per customer confirmation, appliance need to be configured based on that.

ii. Initial Configuration and Licensing

iii. Need to create the basic policy rules and actions as per customer requirement.

3/7/19

7.1.1 UAT for SSL Visibility:

i. Testing with policy, rules and actions

ii. Customer verification and performance testing

7.2 Antivirus & Endpoint detection Response:

7.2.1 Endpoint Protection Manager for AV/HIPs:

i. Bidder need to verify the pre-requisites, deploy the windows OS in VM for Endpoint protection Manager to configure and manage all the endpoints in single point with centralise manner

ii. Create the policies based on customer requirement for malware detection, advance threat detection, IPS etc.

iii. HIPS and Endpoint protection can managed via endpoint protection manager

iv. Need to integrate Endpoint protection Manager with Active directory, DNS and SMTP

v. Creating the alert and report query based on customer requirements, then deployment to all the endpoints

7.2.2 UAT for Endpoint Protection Manager:

i. Check the dash board alerts and data update.

ii. Report generation.

iii. Reflection of endpoints and agent communication checkup.

iv. Daily update and server task checks.

7.2.3 ATP Virtual Appliance Deployment:

i. Bidder need to verify the requirements and deploy the Advance Threat protection Virtual appliance in the VM environment as per requirement.

ii. Integrate ATP with Enpoint protection manager for enhancing the event information and providing endpoint Detection and response functionality.

iii. For storing the logs in ATP database need to be installed externally or Internally in the host.

7.3 WAF – Web Application firewall

i. Bidder need to Inspection the appliance delivered.

ii. Rack mount the shipped appliance and Power on the appliance.

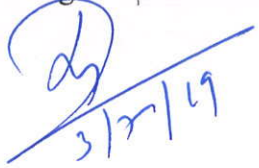
iii. Install the recommended version.

iv. Configure the said management IP addresses.

v. Identify one online application that needs to be protected.

vi. Put the WAF solution in learning mode.

vii. Post 100% learning put the WAF solution in blocking mode.



viii. Apply top 10 OWASP attacks protection policies.

ix. Fine tune the policies applied.

x. Configure Central Management Server to manage WAF appliances for reporting.

xi. Add/configure the L7 DDOS Profile

7.3.1 UAT for WAF:-

i. Check the Policies working in Blocking mode for one application that has been identified.

ii. Minimized false positive if any.

iii. Demonstrate any 2 types of L7 attacks and solution is blocking the same.

iv. Show case that All WAF appliance are discovered and can be managed thru Central Management console for operational activities.

v. Share the Installation guide.

vi. Provide Operational Training on the installation done and configuration done.

8. SIEM –SOW

i. Bidder Verify availability of pre-requisites for SIEM implementation

ii. Base Operating System Installation

iii. Bidder need to Install all connectors/collectors

iv. And Install all components of SIEM solution

v. Integration with IT Infrastructure. For example: Active Directory for logging, Antivirus, all infra devices, collector/logger etc.

vi. Device Integration

vii. Integration with monitoring tool for SIEM components.

viii. Configure SIEM as per requirement

ix. Configure baseline policies SIEM Policies and alerts for production environment.

x. Integrate with threat intelligence cloud of OEM labs and/or as well as third party TI providers if available

xi. Use Cases Development

xii. Configure dashboard reports for alerts configured

xiii. Fine-tuning policies to get filtered alerts

xiv. Prepare SIEM Installation Report

xv. Transition of all infrastructure components to respective operations teams

8.1 UAT/PAC for SIEM

31/7/19

i. Use case testing with support team

ii. Load testing

iii. Performance testing of all modules

iv. Dashboard performance testing

v. Real-time alerting and correlation performance evaluation

vi. Reporting handover to SOC team

9.0 Vulnerability Assessment Management:

i. Bidder need to verify the pre-requisites before deploying Vulnerability manager

ii. Need to deploy in basis of HLD that include the location of Vulnerability manager and database server components, including integration with existing infrastructure system and services

iii. Validate the license

iv. Configure management server and SQL server with centralized policy, event, reporting server and scan job

v. Based on customer confirmation we can perform the activity of agent or agentless scanner for endpoint. Deploy agent only if it required

vi. Create standard operating procedure for asset registration

vii. Assigning asset to required asset groups

viii. Configure the reporting template dashboards as per requirements

9.1 UAT for Vulnerability Assessment:

i. Testing in reports and dashboard alerts

ii. Functionality knowledge transfer to customer

iii. Provide overview on management console, network security scanner, policy event etc.

iv. Create standard configuration document for customer.

Disaster Recovery for DC:

i. Deploy site recovery manager (SRM) and replication manager in both DC and DR

ii. Install and configure the databases for SRM in both sites

iii. Configure the site recovery manager mappings

iv. Deployment of storage replication adopter for storage array based replication for each site recovery manager host

v. Building the protection groups and recovery plans for vm, network, database and storage.

UAT for Disaster Recovery:

3/7/17

i. Perform non-disruptive test for disaster recovery testing

ii. Interactive disaster recovery workshop using virtual infrastructure

iii. Demonstration of backup and recovery of up to two virtual machines using VMware Consolidated Backup

iv. Best practices and knowledge transfer sharing with RAILTEL team

7. Following Clauses of Chapter-3A, SOR-A (Web Application Firewall) may be read as:

SN	Existing Requirement	Modified Requirement
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	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 - Reverse Proxy mode
18	The solution must provide the ability to comply to A+ Certification at the click of a button	The solution must provide the ability to comply to A+ Certification.
22	The solution must have a database of minimally 6000+ signatures that are designed to detect known problems and attacks on web applications.	The solution must have database of enough signature designed to detect known problems and attacks on web applications.
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	The solution must support integration with proposed web application vulnerability assessment tool asked in the RFP.
103	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Web Application Firewalls 2017/2018/2019	The solution must be a Leader or Challenger in the Gartner Magic Quadrant or Forester Leader/Strong Performer of Web Application Firewalls in any year out of 2016/2017/2018 or latest.

3/7/19

104	System must have minimum (fully populated) 6 x10G SFP+ Ports and 2 x 40G ports. Populated Optics should be Multimode.	System must have minimum (fully populated) 6 x10G SFP+ Ports. Populated Optics should be Multimode.
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.	Clause is deleted.
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.	Clause is deleted
127	Should support persistence mirroring and System must support interactive Layer 7 health checks for the application availability	System must support interactive Layer 7 health checks for the application availability

8. Following clauses of Chapter-3A, SOR-B (Backup Solution) may be read as:

SN	Existing Requirement	Modified Requirement
5	Solution Must support Host-Level Virtual Environments Including VMware vSphere, Microsoft Hyper-V	Solution Must support Host-Level Virtual Environments Including VMware vSphere, Microsoft Hyper-V and Guest-Level Virtual Environments including Kernel-based Virtual Machine (KVM).
9	Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Solution must support Advanced sharing of different media across the environment (disk and tape).
15	Solution should offer message level backups for MS Exchange and allow for restore of individual messages or entire folders.	Solution should offer full backup and message level Backup for MS Exchange and allow for restore of individual messages or entire folders
18	Solution must support GUI with centralized management / Single interface for management of all backup and archival activities.	Solution must support GUI with centralized management / Single interface for management of all backup activities.
19	Solution must support Advanced sharing of different media across the environment (disk, tape and optical).	Solution must support Advanced sharing of different media across the environment (disk and tape).
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.	Solution must support following application and database backup with/without CLI for Oracle, 64-bit Active Directory, MS SQL, MS Exchange, Share-Point, MySQL etc.

3/7/17

22	Solution must be able to perform Source (Client) & Target (Backup Server) base block-level de-duplication without requiring expensive and proprietary disk appliances.	Solution must be able to perform Source (Client) & Target (Backup Server) base block-level deduplication with proposed backup solution.
32	Solution should support rapid/instant VM recovery with LiveBoot for Vmware and Microsoft Hyper-V	Solution should support rapid/instant VM recovery for Vmware, Microsoft Hyper-V and KVM.
35	Appliance Should have 2 x 10Gb RJ45 or 2-port SFP+ Network Interface	Appliance should have min. 2-port SFP+ Network Interface fully populated with all optics(multimode).

9. Following clauses of Chapter-3A, SOR-C-i (Virtual Firewall Instance -L3) may be read as:

SN	Existing Requirement	Modified Requirement
1	The solution should be virtual appliance based and enterprise class (complete control from GUI as well as CLI)	The solution should be virtual appliance based and enterprise class (complete control from GUI and CLI/Device Manager)

10. Following clauses of Chapter-3A, SOR-C-ii (UTM) may be read as:

SN	Existing Requirement	Modified Requirement
2	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI as well as CLI)	The UTM/NGFW should be Hardware based and enterprise class (complete control from GUI and CLI / Device Manager).
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	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. Proposed platform should additionally support 8 x 10G SFP+ ports in future
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.	Firewall should provide at least 2 Gbps of NGFW/ Threat Prevention Real world performance (includes FW, Application Visibility, IPS & Anti-Malware) from day one.
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	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	The Firewall solution should support NAT64 & DHCPv6
50	High Availability Configurations should support Active/Active / Clustering, Active/ Passive	High Availability Configurations should support Active/Active / Clustering or Active/ Passive. Bidder has to supply both boxes with stand alone licenses.

3/7/19

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	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. Proposed Solution should include dedicated on premise Sandboxing appliance for static and dynamic analysis of files. Sandboxing appliance should support 2x10G interface and integrated redundant power supply.
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	Clause Deleted

11. Following Clauses of Chapter-3A, SOR-C-iii (Firewall Manager) may be read as:

SN	Existing Requirement	Modified Requirement
1	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	The management platform must be accessible via a web-based interface.
6	The management platform must domain multi-domain management	The management platform must support multi-domain management
14	The centralized management platform must not have any limit in terms of handling logs per day.	The centralized management platform must have minimum 500 GB of local storage for handling logs.

12. Following Clauses of Chapter-3A, SOR-D-i (Commercial SOC includes software components SIEM) may be read as:

SN	Existing Requirement	Modified Requirement
1	The solution must be a Leader in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2017/2018	The solution must be a Leader or Challenger in the Gartner Magic Quadrant of Security Information and Event Management (SIEM) 2016/2017/2018 or latest
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.	The proposed solution should be able to handle 10,000 sustained EPS and/or flows per sec and also data burst/spike upto 15,000 EPS and/or flows per sec without dropping or quing any event from day one. Also shall be scalable to 80,000 EPS in future.
9	The Bidder will give the hardware sizing for the EPS count required since the solution is software based.	The Bidder will provide all the hardware and all required OS and Database for the EPS count required based on the HA in Active-Active running in DC and DR. Complete SIEM solution (hardware, software and storage) to be vetted from SIEM OEM.
ADMINISTRATION AND CONFIGURATION:		

3/7/19

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.	The solution must support the automatic update of configuration information via a centralized management console with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Also detail the features that are updated.
OPERATIONAL REQUIREMENT:		
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.	The solution should mandatorily support high availability requirements at log collection layer with complete solution instance at each DC & DR and without the need for additional 3rd party software to provide 24x7 availability and fault tolerance.
ARCHITECTURAL REQUIREMENT:		
3	The solution must installs on commodity hardware of our choice	Bidder should provide the commodity hardware if solution is software based. Complete SIEM solution (hardware, software and storage) to be vetted from SIEM OEM.
4	The solution must provide browser-based UI access for end users (does not require thick client)	The solution must provide browser-based/thick client UI access for end users.
4	The solution must easily expand to support additional demand.	Clause Deleted
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.	The solution must support Disaster Recovery. It should have the provision to run in active/active mode in both DC-DR environment and should have license to run HA (active-active in DC) as well as in HA (active-active) in DR.
Security and Data Integrity of SIEM:		
4	The solution should block-signs events with a digital signature to demonstrate integrity of the indexed data	The solution should demonstrate integrity of the indexed data
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.	The solution must monitors its own configurations and usage to maintain a complete 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:		

3/7/19

8	The solution should support long term 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.	The solution should support long term access to detailed security event and, if available, network flow data. The system should be able to provide access to at least 3 months online & export capability to external storage.
9	The solution should capture flow information from multiple network points. Solution should support Network traffic collected via TAP, SPAN, and/or Mirror.	Clauses Deleted /part of packet capture
REPORTING:		
27	Dashboard should display asset list and capture details including name, location, owner, value, IP address, platform details	Dashboard should display asset list and capture details like name, location, owner/hostname, value, IP address, platform details etc.
OPEN PLATFORM:		
2	The solution must offers multiple SDKs written on top of the API for:	The solution must offers multiple SDKs written on top of the API for programming/ scripting languages like Python/Java/JavaScript/ PHP/Ruby/C# etc.
2.1.	Python	
2.2.	Java	
2.3.	JavaScript	
2.4.	PHP	
2.5.	Ruby	
2.6.	C#	
CORRELATION AND ALERTING:		
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.	OEM should have integration capability support and this is our future requirement.

13. Following Clauses of Chapter-3A, SOR-D-ii & iii (Anti-Virus +EDR (Client & Server)) may be read as:

SN	Existing Requirement	Modified Requirement
20	Shall offer customizable & standard notifications via - SMTP, SNMP, Pager, NT Event Log	Shall offer customizable & standard notifications via - SMTP, SNMP, NT Event Log
28	Solution must provide virtualized environment	Proposed solution should have the ability to Hunt for threats by searching for indicators of compromise across all endpoints in real-time.
31	Solution must provide to create classify applications which are attempting network access, and block unauthorized	Proposed solution should ensure complete incident playback with continuous recording of endpoint activity, view specific endpoint processes.

31/7/17

	connections and data transfers by malicious programs.	
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	Proposed EDR solution should automatically identify and create incidents for suspicious scripts and memory exploits.
40	Solution must provide to send endpoint logs based on IP and MAC address automatically up to CMAS.	Clause Deleted
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.	The solution should provide for the prevention of access to application data files
47	OEM/bidder must provide RCA (Root Cause Analysis) report of technical problem/ incidence / issues reported and resolved.	Server Security solution should have application and device control to lock down configuration settings, file systems, and use of removable media.
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	Server Security solution should provide predefined automated responses to events. Actions should include alerting the administrator, disabling the user account, logging the event and executing commands/scripts/programs. Solution should have Alerting via file output.
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.	Solution should perform log analysis, integrity checking, root kit detection, time-based alerting and active response. It should help to detect attacks, software misuse, policy violations and other forms of inappropriate activities. Solution should be able to monitor multiple systems, with centrally managed server and the agents that report back to the server.

14. Following Clauses of Chapter-3A, SOR-D-iv (Vulnerability Assessment Software Solution) may be read as:

SN	Existing Requirement	Modified Requirement
1	The scanning solution must be Software / Appliance based, that is deployable in windows and Linux platforms	The scanning solution must be Software / Appliance based, that is deployable in Windows/Linux platforms
13	The Signature database must be exportable to CSV, PDF etc	The Signature database must be exportable to CSV or PDF etc
31	The solution Must provide a graphical, interactive and search friendly topology of the discovered assets	Clause Deleted

3/7/19

41	The Solution must show scan progression and partial scan results in case of large scans	The Solution must show scan progression scan results in case of large scans
52	Solution should allow users to customize the dashboard	Solution should allow users to customize the dashboard. Customization should include filters to allow selection of date ranges, scoping to specific targets/target groups etc.
61	iii) Identify vulnerabilities with zero day	Clause Deleted
	vi) Identify vulnerabilities with high lateral movement	Clause Deleted
	vii) Identify vulnerabilities of type Malware, Trojans	Clause Deleted
64	The solution must allow a way to have N level failover for scanners so that any available scanner picks up the job	The solution must allow a way to have failover for scanners so that any available scanner picks up the job.
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.	The solution must offers integrated password management integration with CyberArk/ PowerBroker Password Safe as well as it includes a built-in third party password management connector.
75	The solution must automates policy definition and policy life cycle management	Clause Deleted
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.	Clause Deleted

15. Technical Specifications for SOR-D-v (Application Black Box Scanner) may be read as:

SN	Technical Specifications
1	Product Must be Leader in Gartner magic Quadrant report at least once in last 3 years.
2	The solution shall support simultaneous Crawl & Audit during scans.
3	The solution shall provide a built in scan profiler to assist in tuning the scan configuration to a target server to improve the effectiveness and accuracy of the scan.
4	The solution allows for real-time review and investigation of vulnerabilities found while a test is still in progress.
5	The solution offers the capability to pause a scan for continuation at a later date without the loss of data.
6	The solution offers the capability to schedule a single or multiple recurring scans in advance.
7	The solution has the capability to maintain false positive tags across scans
8	The solution supports Web Services security testing.
9	The solution provides REST/URL Rewriting (Variable) detection and support.
10	The solutions allows custom checks to be added
11	The solution comes with an array of out-of-the-box scan policies and all major compliance reports which may be further added to and customized.

3/7/17

12	The solution provides the ability to compare and report on two different scans to enable a delta analysis, including a visual representation of vulnerability differences between the two scans and the ability to drill-down into the differences.
13	The solution allows for a re-run of the entire scan with the same settings
14	The solution provides a shortcut to quickly re-test all vulnerabilities
15	The solution provides automatic vulnerability signature updates via the internet. Updates may also be performed manually for offline machines.
16	The solution integrates with a defect-tracking system for easy creation of defects from within the solution itself.
17	The solution must support deployment on-premises, in the cloud and a combination of the two.
18	The solution has the capability to export scan data for upload to a web management console, to be correlated with security vulnerabilities found from static and real time testing. This offers a holistic view of the security status of applications and projects within an enterprise.
19	The solution shall have the ability to feed details of vulnerabilities found during a scan into Web Application Firewall and/or Intrusion Prevention Systems to block potential application exploits
20	The proposed solution must be able to record macros against Web 2.0 applications
21	The solution integrates and works out-of-the-box with a real-time application security technology within Java and .NET servers to: i. Gather internal, code-level vulnerability information by observing the attacks in the code as they happen in real-time. ii. Inspect parts of the application that it may not find through normal crawling iii. Collect information about the internal behaviours of a target application during dynamic tests iv. Detect new types of vulnerabilities, e.g. privacy violation and log fogging. v. Provide stack trace and line-of-code detail during dynamic web application scanning.
22	Skip an attack while the scan is in progress
23	View the actual attack during a scan session

16. The specifications of Packet Capture given in SOR-D-i of Chapter-3A may be read as separate SOR-D-vi. Following Clauses of SOR may be read as:

SN	Existing Requirement	Modified Requirement
5	The solution should have capability to integrate with SIEM to have unified visibility.	The solution should have capability to integrate with proposed SIEM in RFP to have unified visibility.
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.	Proposed solution should Include 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. The proposed Sandbox should have following feature: i) The Sandbox solution must support capability to detect both known and unknown malware behaviours. ii) Full malware lifecycle analysis must be supported so as to fully capture and understand the behaviour of the malwares iii) The Sandbox solution must be able to work with , endpoint security systems , email and web security systems . iv) The Proposed solution must provide a detailed analysis of the effect of the malware on the affected systems.

3/7/17

		v) A hash of the malware should be created for tracking purposes and should support MD5 and SHA256 lookups. vi) The Proposed sandbox solution must have minimally support for Windows OS. vii) The Solution must simulate task in run-time environment to detect more malicious behaviour. vii) The Sandbox solution must Support of analysis of file size of up to 100MB. ix) The solution must support to create the custom environment of RAILTEL, for sandboxing. x) The proposed sandbox solution should allow user to interact/submit the sample within the analysis environment while the analysis is taking place. xi) The solution must integrate with Analytics solution for forensics
24	Should capture signature/heuristics and behavioral based alerts and block the malicious activity	Clause Deleted
27	The Solution must maintain the integrity while sending SSL traffic.	Clause Deleted
28	Solution must support provision to implement custom environment.	Clause Deleted
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	Clause Deleted
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.	Clause Deleted
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.	Clause Deleted
35	Should have minimum 6 x 1 GbE interfaces and 128 GB RAM.	Should have minimum 6 x 1 GbE interfaces and 128 GB RAM. Packet capture solution must have 40TB Storage and scalable to 120 TB.

17. Following Clauses of Chapter-3A, SOR-E-i (Rack Server) may be read as:

31/7/17

SN	Component	Existing Requirement	Modified Requirement
1	General Requirement	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates, system drift detection and secure erase security features inbuilt.	Security: Server should have Hardware (Silicon) root of trust, Cryptographically signed firmware updates features inbuilt
		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 Open Manage server console	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, 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 Open Manage server console
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".	Clause deleted
5	Configured CPU	Should be populated with 2nos. of Intel Xeon Skylake CPU architecture, each CPU should be 16 core 2.3Ghz or more.	Configured CPU Should be populated with 2nos. of Intel Xeon Skylake CPU architecture or latest, each CPU should be 16 core 2.3Ghz or more.
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.	2 nos. of 240GB BOSS card or SATA/SAS SSD in mirrored configuration for OS & 3 nos. of 960 GB SAS SSD and 6x2.4 TB 10k rpm SAS drives.
11	DVD writer	DVD RW	Clause is deleted
13	Ethernet ports	2 x 1G RJ45 and 2 x 10G SFP+ populated with Multimode Transceivers.	2 x 1G RJ45 and 4 x 10G SFP+ populated with Multimode Transceivers.

3/7/17

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	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, 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
23	Server Security	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	Should provide effective protection, reliable detection & rapid recovery using: - Hardware Root of Trust - Signed firmware updates - Secure default passwords - Configuration and firmware updates. - Persistent event logging including user activity - Secure alerting - Automatic BIOS recovery - Rapid OS recovery - System erase

3/7/19

25	Warranty	03 years On-site comprehensive warranty with 24x7x365 remote hardware support.	03 years On-site comprehensive warranty with 24x7x365 embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated case log(portal). It is should be trackable in online portal.

18. Following Clauses of Chapter-3A, SOR-E-ii (10G Switch) may be read as:

SN	Existing Requirement	Modified Requirement
5	The switch quoted should be part of latest Gartner's Leader Quadrant for Data Center networking	The switching OEM should be part of latest Gartner's Leader Quadrant for Data Center networking

19. Technical Specification of SOR-E-ii of Chapter-3A under Software Define Storage For DR may be read as Technical Specification of SOR-E-iii of Chapter-3A (Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License):

20. Software define Storage for DR may be read as Cloud and Software Define Storage.

21. Following Clauses of Chapter-3A, SOR-E-iii (Software defined Storage, Virtualization Virtual Cloud Foundation & Site Recovery License) may be read as:

SN	Existing Requirement	Modified Requirement
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.	The solution should provide broad ecosystem to flexibly deploy on-prem on certified hardware from major OEM vendors and should support service integration with Meity empanelled CSP.
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.	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, uninterrupted service delivery within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and storage virtualization technology.
18	The network virtualization should provide distributed in-kernel routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2	The network virtualization should provide integrated OSPF & BGP features and logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, 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).	& L3 VPN services, distributed L2-L4 stateful in firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration).
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.	Solution provide traffic visibility, 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
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	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
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	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.
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	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

22. Heading of SOR-E-iii "Solution for DR" may be read as Digester Recovery Automation Solution:

23. Added new specifications for Site Recovery under SOR-E-iii (Software defined Storage, Virtualization Virtual Cloud Foundation& Site Recovery License):

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.

3/7/17

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.

3/7/17

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

24. All other clauses of technical requirement for all SOR's will remain same.

The last date of submission of bids is extended from 10.07.2019 to 12.07.2019 up to 15.00 Hrs. Tender will be opened at 15:30 Hrs. on 12.07.2019

All other term & conditions of tender documents will remain same.

3/7/19

(A.K. Sablania)
Executive Director/DNM