TECHNICAL SPECIFICATIONS

CENTRALISED INVENTORY MANAGEMENT SYSTEM (CIMS)

Ser No.	Specifications	Compliance (Yes/No)	Remarks
1.	**Requirement Analysis**		
	(a) Centralised Inventory Management System (CIMS) is a turnkey project. The aim of the subject procurement is to have a proper accounting of stores from its procurement to its condemnation and thereafter procurement of its replacement which must have a paperless functioning of the entire inventory management system.		
	(b) Vendor to analyse present system in Assam Rifles and user requirements to arrive at a proposed solution for the system in terms of Software characteristics. The deliverables in this Phase would include (i) Analyse the present system to understand the short comes and thereafter to study user requirements. (ii) Defining the proposed system in detail. (iii) Preparation of implementation plan. (iv) Approval of implementation by HQ DGAR. (v) Revise the plan as required. (vi) Implementation of final plan after due approval from HQ DGAR.		
2.	**High Level Design**		
	(a) The Software presently in being developed only for Signals Communication Equipment. However in future, HLD should have a provision for subsequent expansion to include stores of other branches that deal with Civil Engineering stores, Clothing, Arms/amn, veh & its spare parts, Rations and other war like stores. (b) Vendor will provide the following on approval of implementation plan. (i) Build Functional Data Model (ii) Build Functional Process Model (iii) Define System performance criteria (iv) Define Architectural Standards (v) Build Prototype (c) Prepare Functional Specifications for each Unit (module) Process.		
3.	**Low Level Design**		
	(a) Do the detailed design of the Software components. (b) Write specifications of various software components based on High Level Design. (c) The Function design documentation should allow the user to approve the description of each Unit Process		

	and contain sufficient details to allow the development Team to process with System Construction activities. The Phase includes following activities: (i) Build Physical Data Model (ii) Build Physical Process Model		
4.	**Platform and Database Agnostic**		
	(a) It would also be required that the application provider should be able to deliver application on latest IT Infrastructure & system software components		
	available at Data Centre, Laitkor. Vendor would ensure that the application developed can overcome the technology dependencies and be available to a variety of user access the network.		
5.	**Software Engineering Standers**		
	It is important that software engineering standards are adopted during the initial stages of the development lifecycle to ensure that the developed solution is able to meet quality certifications and security testing. Following certification would be produced (a) CMM level 3.0 or better for software devp. (b) Third party evaluation certificate from CERT certified evaluators.		
6.	**Software Development : The Software Developed should have**		
	(a) Platform Multi-level independent design		
	(b) AR defined multi-level user privileges and access.		
	(c) Password encryption for access control		
	(d) Multi-user level access of the menu tools and reports		
	(e) Viewing the report in web browser		
	(f) Explorer style data view		
	(g) Exporting old data in a separate archive database		
	(h) Using resource file		
	(j) Dynamically generating Error Log File		
	(k) Separate tools for recovery of the database in case of corruption of the database.		
	(l) MIS report available to selected user only		
	(m) System schedule to perform automatic backup on every day basis.		
	(n) Adequate provision of complete data security.		
7.	**Construction, Compilation and Testing**		
	Produce Unit tested Software components. This include following activities: (a) Program Physical Data Model (b) Program Physical Process Model (c) Prepare User guides and documentation (d) Conduct Unit Testing with demo data.		
8.	**Dashboards**		
	(a) As a senior management tool, most senior officers require dashboards to review total holding of stores, its deficiency, serviceability state, service progress, service levels escalations, alerts and		

	reminders, massages etc. (b) As an operational tool it is required by the office staff for work-list detailing, alerts, reminders and messaging. (c) As configurable component, it would ensure that the user is able to see his role based dashboard for summary of tasks and activities to be completed.		
9.	**Training, finalizing implementation.**		
	(a) **Inital Training**. On successful implementation, proper training on all modules will be provided by the vendor as per plan and schedule provided by HQ DGAR. The training will consist of the following : (i) Hands-on Training during implementation. (ii) On successful implementation, first phase of formal training will be provided for 10 working days for persons of Assam Riffles at Shillong. (iii) Package will be handed over in running condition. (iv) Hand – holding during entire warranty period.		
	(b) **Refresher Training**. There will be five refresher trainings after initial training at the gap of six months. The duration of each refresher training will be for 10 working days for persons detailed by HQ DGAR.		
10.	**Backup of Data**		
	(a) The complete solution should be installed, available and controlled at/ from DC location ie HQ DGAR. Data access should be available upto Battalion level using Assam Rifles network.		
	(b) The complete backup of the system must be available at DR location ie ARTC&S, Sukhovi and regular backup must be updated on daily basis.		
11.	**Documentation**		
	(a) Providing Detailed documentation for managing system technically and at User Level. (b) Documentation to include Technical Documentation & User Manual for the Entire Developed System. (At least one hard and one soft copy of the same to be made available to Assam Rifles Signal Unit and HQ DGAR each. (c) The source code of complete solution with all relevant programmes to be handed over to HQ DGAR after successful implementation of the solution.		

12.	**Solution Sizing and Scalability**		
	Since the solution will be required to be hosted on various deployment models, it is important for the solutions to be able to scale up to meet increasing usage requirements. Although an initial estimation of the hardware specification (quantity and model/version) would be required to size the solution based on system interaction, to increase capacities the solution should be adaptable to scaling. The following should be kept in perspective. (a) Solution should be able to handle increasing number of first time users, transactions, data sharing processes etc. (b) Solution should be able to handle increasing number of concurrent users, concurrent transactions, synchronous data sharing with other systems etc. (c) Solution should be able to perform to the agreed service levels regardless of the bandwidth available or in multiple bandwidth availability scenarios. (d) Solution should be easily scalable to other branches even though they have different products in their inventory. (e) Solution should optimally use technical resources such as memory, processor (CPU), storage etc. In addition should optimally use data centre resources on available bandwidths.		
13.	**Application design for occasionally connected systems**		
	For the small percentage of functionality that requires "occasional disconnected /offline" operations, applications may be designed to use a local persistent store/cache just for the purposes of offline capability and later sync as and when connectivity is restored.		
14.	**Legacy Integration – Digitization & Migration**		
	(a) The solution should provide for manual data entry of legacy data (allow for conduct of digitization activities).		
	(b) Solution should support migration legacy data through be-spoke utilities which allow for data entry, extraction and submission of data into the proposed solution.		
15.	**Intellectual Property Rights**		
	(a) The Intellectual property Rights for the developed product will reside with Assam Rifles. This should include the source code, release management artifacts and all other technical and domain related documentation for the developed solution which will be handed over in softcopy to Assam Rifles on completion of project. The licenses procured for the implementation of the existing application will be provided to Assam Rifles. The software developed should not depend on any propriety basic software for which annual license fee is required to be paid by user. Also, any license required during warranty period will be		

	provided by the vendor at his own cost.		
	(b) The IPR for the developed product / solution should not be restricted / compromised through any legal interpretation. The solution should unambiguously be the property of Assam Rifles.		
	(c) The vendor shall provide at his cost everything necessary for the proper execution of the project according to the intent, requirements and Specifications taken together whether the same may or may not be particularly necessary shown or described therein provided that the same can reasonably be inferred there from.		
16.	**Free Issue Materials**		
	(a) All materials or equipments supplied by the Customer for use in the Contract shall be kept by the Contractor strictly for use in the Contract and shall not be re-allocated to any other work whatsoever without the prior consent in writing of the Customer.		
	(b) All materials or equipments so supplied shall remain the property of the Customer. The vendor shall at all times and places until completion of the Contract, keep and maintain such material and equipment under proper conditions.		
	(c) The vendor shall be liable for all loss or damage however caused to such material and equipment throughout the whole of the period during with they are in its custody and until return to the Customer.		
17.	**Store Management System**		
	(a) The entire system should be deployed on ARWAN and should be accessible over ARWAN to all locations of AR. The data accessibility has to be optimized for minimum bandwidth consumption using Caching at Local Systems and server side processing.		
	(b) The entire system will be deployed centrally through which branch/ HQs/Units can utilize its computing power of their localized system and get the benefits of the Centralized Inventory Management System.		
	(c) The system should store a Centralized Database which is to be used by branch/ HQs/Units as per access rights granted by HQ DGAR		
	(d) The system should have option to create users		
	(e) The system should have different levels of users Admin Level Users & Data Entry Level Users		
	(f) The system should allow different privileges fo different levels of users		
	(g) The system should allow admin level user to access MIS module		
	(h) The system should have option to add/modify/delete units/formations details		
	(j) The system should have option to add/modify/delete branch details		
	(k) The system should have option to authenticate users		
	(l) The system should have option to store/ add/ modify/ delete item category details		

	(m) The system should have option to store accounting units for items		
	(n) The system should have option to store Item Master Details		
	(o) The system should have option to store Vendors details		
	(p) The system should have option to add Store details		
	(q) The system should have option to store supply order details.		
	(r) The system should have option to store serial number/ registration number of the item (if available) along with make and model of the store.		
	(s) The system should have option to store items under expendable category.		
	(t) The system should have option to store its life cycle and must indicate the date of condemnation of the equipment based on life cycle.		
	(u) The system should have option to store details of warranty period / AMC details.		
	(v) The system should have option to store its serviceability status and repair status.		
18.	**Receipt of Stores**		
	(a) DRS: - When store will be received, DRS will be prepared		
	(b) Depot Receipt: - If store receipt from depot, firstly DRS will be prepared and then item will be taken charge on RV		
	(c) **Local Purchase**: - When store receipt from firm, DRS will be prepared and item will be taken charge in CRV		
	(d) **Merge Issue**: -		
	(e) In case cancellation required due to non-collection of item or any other reason, then the issue store to be merged with depot stock and taken on charge by means of CRV		
	(f) **Master Date Record**: - Should have record of all the units and option for addition of new unit		
	(g) **Unit Master**: - For adding new unit		
	(h) **Item Master**: - After receipt the new introduced item which are not in the existing inventory add the item		
	(j) **Due Out**: - All the Dues out item wise, unit wise to be added in master record.		
	(k) **Dues In**: - All the item dues in item wise and vendor wise to be added		
	(l) **Vendor**: - Name of all the firms to be included and on receipt of item		
	(m) **Cost and Date of Purchase** :- Cost of each item and date of purchase to be included		
	(n) **Project case file** :- Each item to include project case file number under which it has been procured		
	(o) **Rejected Stores**: -		
	(p) Details of all the rejected stores to be included in the master date record		
19.	**Section**		

	(a) For addition of new section		
	(b) **Depot**: - For addition of new depot		
	(c) **Casting Error Account Card**: -		
	(d) When any error in Account Card these option are use		
	(e) **Annual Stock Taking**: -		
	(f) The stock taking List for annual stock taking should be generated by the package		
	(g) The system should have option to generate issue vouchers for new demand.		
	(h) The system should have option to generate demands for issue to required items		
20.	**Issue of Store**		
	(a) When the unit demand is being controlled the package should reflect the particular item stock, MSP, Dues in, Dues out, critically of store if stores are available issue stores otherwise dues out to be maintained automatically. In one voucher six item to be printed as well as operator should have flexibility to increase or decrease the item		
	(b) When stores are issued against the dues out maintained on receipt of stores, further part voucher to be generated automatically		
	(c) Package should have option for two types of voucher, regular and further part voucher.		
	(d) Issue registration progress sheet (IRPS) should be printed as and when vouchers are generated. The IRPS sheet should be automatically seen at stores shed and traffic computer		
	(e) The system should manage the dues out automatically		
	(f) **Dues out Clear**: - When store receipt from depot or firm store are taken on charge. Package should reflect automatically dues out if any when receipt is taken on charge		
	(g) **Dues out Renew**: - package should prompt as and when renewal of Dues out is required		
	(h) **Dues out Cancel** :- When unit move out of dependency then all dues out item wise are cancelled and cancellation cert is generated which can be taken on electronic media along with soft copy and other units are enable to retrieve Data for issue/ maint dues out against the unit		
	Issue-in-Lieu: - Option to be included in the package		
	(k) **Transfer Unit Dues Out**: - The dues out of station, stores to be automatically transferred to the new incoming unit		
	(l) **Dues Out Upgrade**: - Option for up gradation of dues out quarterly/ Annually to be included		
	(m) The system should be able to carry out review based on the issue/receipt and MSP of all items to be fixed by software application before finalization of Annual		

	Procurement plan		
	(n) The option for accounting of salvage stores to be included manually procedure followed has been studied and requirement noted by the firm reps		
	(o) The system should have option to receive item for repair from units and other branches		
	(p) The system should have option to send items to vendors for repair		
	(q) The system should have option to receive items from vendors after being repaired		
	(r) The system should have option to return item to respective unit after repair		
21.	**Reports Generation**		
	(a) The system should generate stock report of all the items.		
	(b) The system should generate available stock report for the list of items		
	(c) The system should generate report for the list of items issued, date wise, unit wise ,etc.		
	(d) The system should generate notification if the demand is not processed for certain period of time		
	(e) The system should generate report for the list of items received for repair		
	(f) The system should generate report for the list of items given for repair		
	(g) The system should generate report for the list of item received after being repaired		
	(h) The system should generate report to show the list of stores issued.		
	(j) The system should generate report to indicate expiry of warranty / AMC		
	(k) The system should generate report to indicate expiry of life cycle		
	(l) The system should generate report for deficiency of given items as per authorisation of Assam Rifles		
	(m) The system should generate report giving details of unserviceable/ under repair items		
	(n) **Reports to be Printed**		
22.	**Print of Account Card**		
	(a) System should have facility to prepare and print customized report based on any combination of above		
	(b) Print Account card all items		
	(c) Print Account Card only for transaction made		
	(d) Dues out all items particular unit (LCC)		
	(e) Dues out all particular item all units		
	(f) Dues out all items particular unit		
	(g) Dues out particular unit particular item		
	(h) Dues out all items particular unit (expandable)		
	(i) Issue particular item all units		
	(j) Issue particular item particular unit		
	(k) Issue particular unit all items		

	(l)	Issue details all items (LCC)		
	(m)	Issue details all items (Expandable)		
	(n)	Receipt particular item from all depot		
	(o)	Receipt from LP of particular item		
	(p)	Receipt from all depot particular section		
	(q)	Receipt details all item particular period		
23.	**Printing of Maintenance Report**			
	(a)	Details of issue per day		
	(b)	Details of receipt per day		
	(c)	View inventory details		
	(d)	Surplus inventory details		
	(e)	Deficient inventory details		
	(f)	Non-moving items		
24.	**Printing of details of Dues in items from various firms**			
	(a)	List of item dues In from firm		
	(b)	List of item where delivered period expired		
	(c)	More than one year		
	(d)	More than six month		
	(e)	More than three month		
	(f)	Less than three month		
	(g)	List of receipted vouchers pending from units for specified period.		
HARDWARE SPECIFICATIONS				
25.	**High End Switch**			
	(a)	**Architecture**		
		(i) Modular architecture, minimum four slots for interface modules		
		(ii) Shall have two dedicated management module slots in addition to the interface modules		
		(iii) Shall have CLOS Architecture or equivalent shared (iv) switch fabric capability with minimum four switch fabrics all supporting active switching to support high switching capacity		
		(v) Shall have fully distributed architecture (any additional hardware required for the same shall be proposed before technical evaluation and any changes after that will be provided additionally by vendor at his own cost)		
		(vi) Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all line cards (any additional hardware required for the same shall be proposed before technical evaluation and any changes after that will be provided additionally by vendor at his own cost)		
		(vii) Shall have minimum 3.2 Tbps of switching capacity or higher		
		(viii) Shall have 8 x10 G SFP+, 16 x1 G-SFP and 48x10/100/1000 Base T ports functional from day-1		
		(ix) Shall be 19" Rack Mountable		
		(x) The Switch should have inbuilt/ pre-loaded operating system with modular architecture		
	(b)	**Advanced Service Modules support**. The switch		

	shall support service modules to port applications directly to the switch chassis. This shall include support VPN Firewall module		
	(c) **Resiliency**		
	(i) Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 router		
	(ii) Shall support virtual switching fabric creation across four chassis-based switches using 10G Ethernet Links		
	(iii) Should support Virtualizes a physical switch into multiple logical devices, with each logical switch having its own processes, configuration, and administration		
	(iv) Should support Hot-swappable Modules		
	(v) Passive backplane with no active components for increased system reliability		
	(vi) IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol		
	(vii) IEEE 802.3ad Link Aggregation Control Protocol (LACP)		
	(viii) Ring protocol support to provide sub-100 ms recovery for ring Ethernet-based topology		
	(ix) Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments		
	(x) Graceful restart for OSPF, IS-IS and BGP protocols		
	(xi) Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP protocols		
	(x) The Switch support In-Service Software Upgrade (ISSU)		
	(d) **Layer 2 Features**		
	(i) Shall support up to 4,000 port or IEEE 802.1Q- based VLANs		
	(ii) Shall support GARP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs		
	(iii) Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected,preventing loops		
	(iv) Shall support IEEE 802.1ad QinQ and Selective QinQ to increase the scalability of an Ethernet network by providing a hierarchical structure		
	(v) Shall support Jumbo frames on GbE and 10-GbE ports		
	(vi) Internet Group Management Protocol (IGMP)		
	(vii) Multicast Listener Discovery (MLD) snooping		
	(viii) IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		

	(ix) Multicast VLAN to allow multiple VLANs to receive the same IPv4 multicast traffic		
	(e) **Layer 3 Features (any additional licenses required shall be included)**		
	(i) Static Routing for IPv4		
	(ii) RIP for IPv4 (RIPv1/v2)		
	(iii) OSPF for IPv4 (OSPFv2)		
	(iv) IS-IS for IPv4		
	(v) Border Gateway Protocol 4 with support for IPv4 addressing		
	(vi) Policy-based routing		
	(vii) Unicast Reverse Path Forwarding (uRPF)		
	(viii) IPv4 tunneling to allow IPv4 packets		
	(ix) Dynamic Host Configuration Protocol (DHCP) client, Relay and server		
	(x) PIM Dense Mode (PIM-DM), Sparse Mode (PIM- SM), and Source-Specific Mode (PIM-SSM) for IPv4 multicast applications		
	(xi) MPLS and VPLS Support		
	(xii) Should support PBR, OSPF, BGP, NSF, MPLS, VPLS from day one		
	(xiii) Should support Virtual Extensible LAN (VXLAN) with the help of additional line card		
	(f) **QoS and Security Features**		
	(i) Access Control Lists for both IPv4 for filtering traffic to prevent unauthorized users from accessing the network		
	(ii) Port-basedrate limiting and access control list (ACL) based rate limiting		
	(iii) Congestion avoidance using Weighted Random Early Detection (WRED)		
	(iv) Powerful QoS feature supporting strict priority (SP) queuing, weighted round robin (WRR) and weighted fair queuing (WFQ)		
	(v) IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port		
	(vi) Media access control (MAC) authentication to provide simple authentication based on a user's MAC address		
	(v) Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers		
	(vi) Port security and port isolation		
	(g) **Management Features**		
	(i) Configuration through the CLI, console, Telnet, SSH and Web Management		
	(ii) SNMPv1, v2, and v3 and Remote monitoring (RMON) support		
	(iii) sFlow (RFC 3176) or equivalent for traffic analysis		
	(iv) Management security through multiple privilege levels with password protection		
	(v) FTP, TFTP, and SFTP support		
	(vi) Port mirroring to duplicate port traffic (ingress		

		and egress) to a local or remote monitoring port. Shall support minimum four mirroring groups		
		(vii) RADIUS/TACACS+ for switch security access administration		
		(viii) Network Time Protocol (NTP) or equivalent support		
		(ix) Shall have Ethernet OAM (IEEE 802.3ah) management capability		
	(h)	**Environmental Features**		
		(i) Shall provide support for RoHS and WEEE regulations		
		(ii) Shall be capable of supporting both AC and DC Power inputs		
		(iii) Operating temperature of 0°C to 45°C		
		(iv) Safety and Emission standards including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A		
	(j)	**Software Defined Networking (SDN) Capability**		
		(i) The Switch should have Open Flow Open flow 1.3.1 protocol capability to enable software-defined networking from Day one		
		(ii) The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Openflow protocol		

26.	**Unified Threat Management**		
	(a) General Requirements		
	(i) Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
	(ii) The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs'(or equivalent)NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%		
	(iii) OEM should be in Leaders quadrant of Gartner's – in Enterprise Firewall Magic Quadrant (or equivalent) as per the latest report		
	(iv) Appliance shall be ICSA certified for Firewall, IPS, Gateway AntiVirus, IPSec VPN, SSL VPN functionalities		
	(b) Hardware & Interface requirements		
	(i) 14 x 1GE RJ45 inbuilt interfaces, 4 x 1GE SFP interface slots from day one		
	(ii) The Appliance should have 1x USB, 1x dedicated Console Port		
	(c) Performance and Availability		
	(i) The Firewall should be on ASIC Based multiprocessor architecture with minimum 18 Gbps of Firewall throughput for 1518 byte packet size, 2,000,000 concurrent sessions, and 130,000 new sessions per second support from day one and Firewall Latency should not be more than 3µs		
	(ii) Minimum IPS throughput of 5500 Mbps from day one		
	(iii) Proposed solution must support minimum 1 Gbps of SSL Inspection throughput		
	(iv) IPSec VPN throughput: minimum 8 Gbps		
	(v) Simultaneous IPSec VPN tunnels: 500		
	(vi) Should have 200 SSL VPN peer support from day one		
	(vii) Proposed solution must support minimum 10 virtual firewall from day one		
	(d) Routing Protocols		
	(i) Static Routing		
	(ii) Policy Based Routing		
	(iii) The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS		
	(e) Firewall Features		
	(i) Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, IMAP, NFS etc		
	(ii) IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP		
	(iii) Allows secure deployment of next-generation IPv6		

		networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6		
		(iv) The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation		
		(v) The Firewall should support ISP link load balancing.		
		(vi) Firewall should support link aggregation functionality to group multiple ports as single port.		
		(vii) Firewall should support minimum VLANS 2048		
		(viii) Firewall should support static NAT, policy based NAT and PAT		
		(ix) Firewall should support IPSec data encryption		
		(x) It should support the IPSec VPN for both site- site and remote access VPN		
		(xi) Firewall should support IPSec NAT traversal.		
		(xii) Support for standard access lists and extended access lists to provide supervision and control		
		(xiii) Control SNMP access through the use of SNMP and MD5 authentication.		
		(xiv) Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN		
		(xv) The Firewall should have integrated solution for SSL VPN		
		(xvi) Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them		
		(xvii) The solution should have basic server load balancing functionality as an inbuilt feature		
		(xviii) Licensing should be a per device and not user or IP based (should support unlimited users)		
	(f)	**Integrated IPS Features Set**		
		(i) IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.		
		(ii) Support SYN detection and protection for both targets and IPS devices.		
		(iii) The device shall allow administrators to create Custom IPS signatures		
		(iv) Should have a built-in Signature and Anomaly based IPS engine on the same unit		
		(v) Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one		
		(vi) Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)		
		(vii) Signature updates do not require reboot of the unit.		

		(viii) Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems		
		(ix) IPS Actions: Default, monitor, block, reset, or quarantine		
		(x) Should support packet capture option		
		(xi) IP(s) exemption from specified IPS signatures		
		(xii) Should support IDS sniffer mode		
	(g)	**AntiVirus & AntiBot**		
		(i) Firewall should support antimalware capabilities, including antivirus, botnet traffic filter and antispyware		
		(ii) Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family		
		(iii) Solution should be able to block traffic between infected host and remote operator and not to legitimate destination		
		(iv) Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.		
		(v) Solution should have an option of packet capture for further analysis of the incident		
		(vi) Solution should uncover threats hidden in SSL links and communications		
		(vii) The AV should scan files that are passing on CIFS protocol		
		(viii) The proposed system shall provide ability to allow, block attachments or downloads according to file Extensions and/or file types		
		(ix) The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
	(h)	**Other support**		
		(i) Should support features like Web-Filtering, Application-Control & Gateway level DLP from day one		
		(ii) The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million web pages in 72+ categories and 68+ languages without external solution, devices or hardware modules.		
		(iii) Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)		
		(iv) The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.		
		(v) The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System		

	services,. Should support for QoS features for defining the QoS policies.			
	(vii) It should support the VOIP traffic filtering			
	(viii) Appliance should have identity awareness capabilities			
	(ix) The firewall must support Active-Active as well as Active-Passive redundancy.			
	(x) Solution must support VRRP clustering protocol.			
	(j) Management & Reporting functionality			
	(i) Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.			
	(ii) Support accessible through variety of methods, including console port, Telnet, and SSHv2			
	(iii) Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.			
	(iv) Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS			
	(v) The Firewall applaince should have minimum 450GB of internal storage for local reporting			
	(vi) Solution must allow administrator to choose to login in read only or read-write mode			
27.	**Hyper Convergent Infrastructure**			
	Hyper-Converged Solution for Cloud			
	(a) **Analyst Ratings** The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's quadrant in the Gartner Magic Quadrant (or equivalent) report.			
	(b) **HARDWARE AND PERFORMANCE REQUIREMENTS**			
	(i) Offered Hyper-Converged Capacity	The offered appliance shall be based on modular building blocks of up to one compute node. Each block shall be built using a 2U modular chassis / enclosure housing the compute with respective storage capacity. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes		
	(ii)Hardware Support	Solution must be x86 infrastructure agnostic and available to be deployed on a choice of atleast 3 server OEMs		
	(iii)Hyper-Converged Infrastructure	Proposed solution must be based on converged IT infrastructure platform that integrates storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.		
	(iv)Functionality	Proposed hardware must be capable to Deduplicate, Compress & Optimize ALL data inline, in real-time, across all storage tiers: All handled with fine data granularity of 8KB data blocks		
	(v)Hardware Specifications	Each Compute Block must come with the following specifications: Dual Intel Intel® Xeon® Gold 5120 Processor or		

		Dual Intel Intel® Xeon® Gold 5120 Processor or higher Use of All SSD Drives for Caching and Persistent storage. Minimum 5*1.92TB SSD for data storage Minimum 256GB of DDR4 RAM at 2400 Mhz or above 2*40GbE NIC		
	(vi) Resiliency	Proposed solution must be able to support multiple points of failure with no loss of function or data.		
		During a single component failure (of any type) production services are not affected / degraded in anyway		
		Solution will be deployed as a stretched cluster with Zero RTO. Solution should support stretched cluster deployment in a near site metro DC deployment.		
		Each node should have dedicated non-shared dual-PSU's and should be able to sustain single power supply failure. Solution should not utilize micro-server architecture with shared PSU's and other components.		
		Must be able to sustain minimum of simultaneous 2-HDDs failures per node without DU/DL		
		Must be able to sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without DU/DL		
		Must be able to sustain one node failure in the cluster. Must be able to sustain 1 NIC port failure		
	(c) SOFTWARE AND FUNCTIONALITY REQUIREMENTS			
	(i) Common Features Included	The proposed solution must be able to provide enhanced functionality by including the following available without compromise in function or performance in both Hybrid as well as All Flash Nodes:		
		Global dedupe, compression and optimization with minimum impact to production workloads and guaranteed CPU and RAM available to user applications		
		VM-centric policy-based backup/recovery/DR		
		WAN-optimized data protection for VM mobility		
		Unlimited real time data Deduplication Function - licenses Included		
		Unlimited real-time data Compression Function -licenses Included		
		Unlimited capacity Backup Function- Included		
		Should include licenses for multi-site deployments of atleast 3 sites		
	(ii) Global Unified Management	Proposed solution must be able to support the following Global Unified Management features		
		VM-centric management through a single pane of glass via the virtualization manager		
		Programmatic interface to enable automated		

	Recovery	following Data Recovery features		
		Data recovery should be indepent of source Virtual Server		
		Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time		
		Data recovery process should be simple with an RTO in minutes		
	(vi) Disaster Recovery	Proposed solution must be able to support the following Disaster Recovery features		
		The solution must provide a simple failover operation		
		The solution must allow creation of a Runbook to automate recovery of Virtual Servers		
		The solution must allow changing of IP address of recovered Virtual Servers to match target datacenter		
		The solution should allow changing Virtual Server settings (example vCPU, vRAM, VMSwitch) if required		
		The solution must allow the option to test DR failover to separate network with no impact to production workloads		
		The solution should have feature to assist in failback process to Primary datacenter		
	(vii) Private Cloud License	The Proposed solution must be offered with cloud-ready operating system that is ideal for highly virtualized and software defined datacenter environments.		
		It must include Shielded Virtual Machines, software defined networking, Storage Spaces Direct, and Storage Replica; customers receive rights to unlimited Operating System Environments (OSEs)		
		The proposed solution must provide following features: Computing environment: The virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking. Disaster recovery and backup, Optimization.		
		Solution must have features such as live migration, storage migration, and import/export to move or distribute a virtual machine.		
		It must offer a remote connection tool for use with both Windows and Linux.		
		The solution should have Secure boot and shielded virtual machines that protects against malware and other unauthorized access to a virtual machine and its data.		
		The solution must give virtual machine direct and exclusive access to some PCIe hardware devices. Using a device in this way bypasses the virtualization stack, which results in faster access.		

		The solution must prevent a virtual machine's excessive activity from degrading the performance of the host or other virtual machines.		
		A virtual machine can be used as a host and create virtual machines within that virtualized host.		
		The solution must have option to set up Remote direct memory access (RDMA) on network adapters bound to a virtual switch, regardless of whether switch embedded teaming (SET) is also used.		
		The solution must have features to make it harder for virtualisation administrators and malware on the host to inspect, tamper with, or steal data from the state of a shielded virtual machine.		
28.	**Authentication Tokens**			
	(a) Certification	FIPS 140-2 Level 2 or as per CCA Guidelines CC / EAL 4+		
	(b) Asymmetric Key Operations	• PKCS#11 compliant • RSA signature: 2048 bit or higher • Secure hash: MD5, SHA -1, SHA-256, SHA -512 □ ECC P-Curves		
	(c) Memory	64 KB or more		
	(d) Credential Storage	• X.509 V3 certificates, • secure symmetric key storage • Microsoft Windows Credentials		
	(e) Platform Support	Windows7, 10, Windows Server 2012and higher server OS, Linux OS		
	(f) Random Number Generator	ANSI X9.31 PRNG or NIST DRBG SP 800 90 CTR mode		
	(g) Data Transfer rate	125 Kbps or more		
29.	**Barcode Printer**			
	(a) Printer Type	Direct Thermal / Thermal Transfer		
	(b) Processor &	400 Mhz Processor,		
	(c) Memory	min 128 MB Flash, 128 MB SDRAM (standard)		
	(d) Print Methods	Direct thermal and thermal transfer, Printing of barcodes, text and graphics.		
	(e) Resolution	203 dpi/8 dots per mm		
	(f) Print Width	min 4.09"		
	(g) Print Length	min 155"		
	(h) Print Speed	min 6IPS		
	(j) Weight & dimension	not more than 12KG		
	(k) Media handling	6.0" (152 mm) O.D. on a 1" (25 mm) I.D. core		
	(l) Sensors	transmissive sensors & reflective sensor		

	(m) Drivers	linux, Windows 10, Windows 8, Windows 7, Windows Server 2016, Windows 8.1, Windows Server 2012, Windows Vista (32 & 64Bit)		
	(n) Display	Icon-based LCD multilingual graphical user interface and full function keypad		
	(o) Construction and access	Metallic Frame, Bifold Door fo easy access to media		
	(p) Communication and Interface Capabilities	USB 2.0 & RS232		
	(q) Media Spec	Should support min 450 meters ribbon roll		
	(r) Printing language	Should support ZPL, ZPL II, EPL & EPL2		
	(s) Device management	Should be supported by SOTI & Airwatch		
	(t) Cloud printing	the printer Should be able to connect to the Cloud directly and securely, forwarding data from any port.		
	(u) Media handling	Should Support labels with Gap, Mark in roll form; should support fan fold media		
	(v) Input	100-240 VAC, 50-60 Hz		
	(w) Barcode Support	Should Support all 1D and 2D Symblogies		
	(x) Certification	BIS for printer , Energy Star compliant		
	(y) Service Center	OEM should have an ISO certified service center in India for at least 3+ years		
	(z) OEM	OEM should be present in country as a direct entity for min of 5 years and should have sold a min of 50000 barcode printers in India ia and should have a global turnover of over 500 Million for past 3 years (cash flow positive)		
30.	**Barcode Scanner**			
	(a) Technology	Digital imager 2D Barcode scanner		
	(b) Hands free operation	Scanner should operate in hands free mode when placed on stand. Scanner should auto trigger when a barcode is presented		
	(c) Image Resolution	Min VGA (640 x 480) or better		
	(d) Depth of field	min 11 inch for 20 mil QR code for ease of scanning from stand		
	(e) Symbologies	PDF417, MicroPDF417, Data Matrix, Maxicode, QR Code, MicroQR, Aztec. Supports most 1D and 2D Symbologies.		
	(f) Ambient Light Immunity	Scanner should be able read in bright and low light of 0-105,000 Lux (total dark to Bright sunlight)		

	(g) Reading Precision	>=4 Mil code 128 and min 6.7 ,mil QR Code		
	(h) Pitch	Roll Pitch Yaw 0 - 360° ± 65° or greater ± 60° or greater		
	(j) Minimum Symbol Contrast	min 25% MRD		
	(k) Interface	USB		
	(l) Weight	less than 170gms		
	(m) Indication	Beep (adjustable tone) and Visual indication of Good and bad reads		
	(n) Power	Scanner should be powered by USB port. No separate Adaptors should be needed		
	(o) Operating Temperature	0 to 50 degrees Celsius		
	(p) Storage Temperature	-20 to 70 degrees Celsius		
	(q) Humidity	5% to 95% (non -Condensing)		
	(r) Drop & Tumble	should withstand 1.5 meter drop and min 250 tumbles		
	(s) IP Sealing	Min IP42 or above		
	(t) OEM	OEM should be present in country as a direct entity for min of 5 years and should have sold min of 100000 barcode scanners within India and should have a global turnover of over 500 Million for past 3 years (cash flow positive)		
	(u) Warranty	OEM certified 5 (Five) Years onsite 100% comprehensive warranty from Go Live date of Project		
	(v) OEM service centre	OEM should have an ISO certified service centre with in the country operational for min 3 years prior to the tender date		
	(w) Certification	BIS certified		
31.	**Application Load Balancer (Architecture)**			
	(a) Should be high performance purpose built hardware with multicore CPU support.			
	(b) The appliance should have 8 GB RAM and 5 Gbps of system throughput to support multiple load balancing features and functions			
	(c) The appliance should have minimum 4 triple speed 10/100/1000 Mbps Gigabit copper ports & option for 2 * 10G SFP+ ports			
	(d) Solid state drive (SSD) for high I/O performance and dual power supply support			
	(e) Hardware based SSL acceleration with 2Gbps of bulk SSL throughput and 2800 2k SSL transactions per second (TPS)			
	(f) USB based fast failover support for automated configuration synchronization and improved failover time as compare to traditional cluster			
	(g) In order to meet high performance requirements load			

	balancer must support virtual grouping (not clustering) of the appliances and must appear as single system.		
	(h) Multiple appliances in virtual group/domain should allow administrator to configure one or more applications application (virtual services) across both physical appliances to meet high performance requirement		
32.	**Load balancing features**		
	(a) Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support		
	(b) The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header etc.		
	(c) Should support Multi-level virtual service policy routing – Static, default and backup policies for intelligent traffic distribution to backend servers		
	(d) Support for policy nesting at layer 7 and layer 4, solution should able to combine layer 4 and layer 7 policies to address the complex application integration.		
	(e) Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support e-Policies to customize new features in addition to existing feature/functions of load balancer		
	(f) Traffic load balancing using e-Policies should support algorithms including round robin, least connections, shortest response, persistence IP, hash IP, hash IP and port, consistent hash IP and SNMP		
	(g) Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.		
	(h) Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.		
	(j) Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.		
	(k) should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers		
	(l) Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..		
	(m) Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.		
	(n) Should support certificate parser and solution should integrate with client certificates to maintain end to end security and		

	non-repudiation		
	(o) The appliance should support Certificate format as "Open SSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".		
	(p) Should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.		
	(q) Should provide full IPv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for IPv6 phase-2 certification.		
	(r) IPv6 gateway should provide compressive support for IPv6 functions to help with IPv4-to- IPv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT		
	(s) Should support various deployment modes for seamless integration including reverse proxy (IPv6 to IPv4, IPv4 to IPv6) and IPv6 to IPv6 transparent and reverse proxy mode.		
33.	**Network and application security**		
	(a) Should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.		
	(b) Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation.		
	(c) Should support integrated network based firewall to protect against network based attacks; administrator should able to configure the security policies on per interface basis.		
	(d) Proposed solution provide integrated WAF functionality to protect against layer 7 attacks and should support deep packet inspection of HTTP & HTTPS traffic in reverse proxy mode		
	(e) Application firewall should support built in rules to counter application attack, provision should be there to customize predefined application security rules. Should support all kind of attacks including OWASP top 10		
	(f) WAF module should support both detection and prevention mode and policies should be enforced on per virtual services.		
34.	**Clustering and failover**		
	(a) Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support USB based fast failover.		
	(b) should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization, system memory, process health check and gateway health check to support the failover in complex application environment		
	(c) Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway		
	(d) Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.		
	(e) should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to minimize the failover delay		
	(f) Support for multiple communication links for real-time		

	configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc and heartbeat information		
	(g) Clustering function should support IPv6 VIP's (virtual service) switchover		
	(h) N+1 clustering support with active-active and active-standby configurations.		
35.	**Centralized management**		
	(a) Centralized management appliance should have extensive reporting and logging with inbuilt TCP dump like tool and log collecting functionality		
	(b) The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.		
	(c) Should support XML-RPC for integration with 3rd party management and monitoring		
36.	**Network Traffic Manager (BANDWIDTH CONTROLLER)**		
	An additional device for bandwidth control should be provided along with the system. The features are as follows.		
	(a) The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems		
	(b) The system should identify and control bandwidth hogs so that network administrators can identify problem users, applications and websites and apply automated policies to limit or prevent bandwidth allocation.		
	(c) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.		
	(d) **Real-time Monitoring:** The system should monitor the health of network in real time and give insight about how applications are performing, bandwidth consumed by users, applications across the network		
	(e) **Policy-Based Shaping:** The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.		
	(f) **Interactive Analytics:** Intuitive dashboard feature should be there to visualize activities by all users.		
	(g) **Application Acceleration:** The system should support acceleration and caching features.		
	(h) **Predictive Recommendations:** The system should have the feature to study the patterns and trends in the network and automatically make suggestions to repair and improve network performance.		
	(j) **Traffic shaping and Acceleration**		
	(i) Shaping Throughput: - 1 Gbps		
	(ii) Concurrent Flows: - 220,000		
	(iii) Packets per second: - 200,000/s		
	(iv) New Connection Rates: - 10,000/s		
	(v) Acceleration Throughout: - 30 Mbps		
	(vi) Edge Cache Throughput: - 50 Mbps		
	(vii) Optimized Connections: - 6,000		
	(viii) APS Objects 250		
	(ix) SLA Objects 250		
	(x) PDF Reports 60		
	(xi) Traffic Policies 1024		
	(k) **Interface Capability**		

	(i) The system should have 1 x RJ45 based dedicated console port for management purpose.			
	(ii) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future expansion.			
	(I) **Physical Parameters**			
	(i) Form Factor: -1U rack mountable			
	(ii) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)			
	(iii) Environment: - 0 deg C to 40 deg C, 5% to 90% operating humidity.			
37.	**Two units of under mentioned device should provide with the following system.**			
	(a) **SYSTEM PARAMETERS**			
	Speech band	300to 3400Hz		
	Modulation	Pulse Code Modulation		
	No. of channels per system	32 (30 speech channels, 1 terminal Signalingand1Sync.Channel)		
	Sampling frequency	8000 Hz		
	No of sample bits	8 per channel		
	Total bits per frame	256		
	Bit rate	2048 Kbps ± 50ppm		
	Construction and Architecture	Chassis based modular multiplexer Shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic		
	Universal Slots	All slots (other than for power and control)should be universal i.e. capable of accepting any type of voice/ data/ fax card manufactured by the same OEM.		
	Add-Drop or Drop - Insert Function	(a) Should be able to add-drop/ drop-insert voice and data at channel (64 kbps) multiple channel (nx64Kbps) and at E1. (b) Add-drop should be software configurable by user in the field		
	Digital Cross Connection function	(a) It should have an inbuilt cross connect facility on the same equipment (b) Cross Connect: It should be able to map the following voice interfaces: (i) E1 to E1 (ii) E&M (two wire or four wire) toe1 and vice versa (iii) FXO/FXS to E1 and vice versa (b) Add-drop should be achievable by software by user in the field		
	Redundancy	Dual controller, dual power with load sharing		
	Protection	1 for 1 protection, E1, T1, FOM		
		PDH ring protection, QE1, QT1, FOM, MiniQE1, 3 E1 for DS0SNCP protection		
	Management	Console, Telnet, SNMP, and Inband Management support		

		Craft interface port for connection to external LCD display		
		Compatible to a SNMP based GUI network management system		
	No. of Slots	Should have 16 or more hot plug-in slots with capability to support following cards.		
		Single E1/Quad E1 (G.703)/ Mini-Quad E1/3*E1 card-DS0 SNCP protection		
		X.21/V.35/RS232/EIA530		
		2W/4WE&M		
		QFXO/QFXS/12FXo/12FXS/24FXO/2 4FXS		
		10/100 Base-T Router Card		
		2/4 channel G.SHDSL card		
		8-channel Dry Contact I/O		
		TDMoE (TDM over Ethernet) with 2 Combo Giga Bit (GbE) interface for IP uplink		
	(b) Interface Support:- The system shall support below mentioned interfaces/Cards.			
	(i) Network Line Interface - E1 should comply with the following specifications:-			
	Number of ports	4 x E1		
	Line Rate	2.048 Mbps ± 50 ppm		
	Line Code	AMI or HDB3		
	Input Signal	ITU G.703		
	Output Signal	ITU G.703		
	Framing	ITU G.704		
	Connector	BNC/RJ48C, DB25S for Mini Quad E1		
	Electrical	120 ohm twisted pair		
	Jitter	ITU G.823		
	(ii) 2*10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications			
	Number of ports	2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate nx64K bps, 1≤ n ≤32 (≤ 4Mbps for total of all 64WAN ports)		
	Physical Interface	10/100 Base Tx2		
	Connector	RJ45		
	Routing protocol	RIP-I, RIP-II, OSPF, Static		
	Supporting Protocols	PPP(IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP		
	Diagnostic	Ping, Trace route		
	QoS	Rate limit		
	(iii) 8*10/100 Ethernet Router Card with capability to handle 64 WANs			

	Number of ports	8 LAN ports, Max 64 WAN ports. Each WAN port has data rate nx64K bps.		
	Physical Interface	10/100 Base T x8		
	Connector	RJ45		
	Routing protocol	RIP-I, RIP-II, OSPF, Static		
	Supporting Protocols	PPP(IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT,DHCP		
	Diagnostic	Ping, Trace route		
	QoS	Rate limit		
	(iv) Voice Card (8EM) port (interfaces) should comply with the following specifications:-			
	(aa) Connector : RJ45 connector (ab) Alarm conditioning : CGA busy after 2.5 seconds of LOS, LOF (ac) Encoding : A-law or μ-law user selectable together for all. (ad) Impedance : balanced 600 or 900ohms. (ae) Longitudinal rejection: 55dB (af) Loss adjustment : -21 to +10 dB/0.1 dB step transmit and receive (ag) Single/ distortion : >46 dB with 1004Hz, 0 dBm input (ah) Frequency response : -0.25 to -1 dB from 300 to 3400Hz (aj) Signaling : Type1,Type 2, Type3, Type 4, Type5 transmit only			
	(v) Voice card (12FXS/ 12FXO/ 24FXS/ 24FXO) port (interfaces) should comply with the following specifications:-			
	(aa) 12 FXS/ FXO Connector :Twelve RJ11 (ab) 24FXS/FXO Connector :one RJ21X (ac) Alarm conditioning : CGA busy after 2.5 seconds of LOS, LOF (ad) Encoding : A-law or μ-law, user selectable together for all (ae) AC Impedance : balanced 600 or 900 ohms			
	(af) Longitudinal Conversion Loss : >46 DB (ag) Cross talk measure : Max -70 dBm0 (ah) Gain Adjustment: -21 to +10 dB / 0.1dB step transmit & receive (ai) Signal/Distortion : >25 dB with 1004 Hz, 0 dBm input (aj) Frequency Response : -0.25 to -1dB from 300 to 3400Hz, coincide with ITU-TG.712 (ak) Loss adjustment : -21to+10 dB/ 0.1dB step transmit and receive (al) Signal /Distortion: 46 dB with 1004 Hz, 0dBm input (am) Frequency response: -0.25 to -1 dB from 300 to 3400Hz, coincide with ITU-T. (an) Ideal channel noise: Max -65 dBm op			

	(ao) Inter-modulation : coincide with ITU-T B.712 (ap) 2Wire return loss : > 2dB echo, >20 dB signing (aq) FXS loop feed : Nominal -48 V dc with 20 mA Current limit (ar) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse			
	(vi) G.SHDSL Line port (interfaces) should comply with the following specifications:-			
	Number of ports	2 or 4		
	Line Rate for 4 - channel G.SHDSL	nx64 Kbps (n= 3to 31)		
	Line Rate For 2-channel G.SHDSL	nx64 Kbps (n= 3to 15)		
	Line Code	16-TCPAM, full duplex with adaptive echo cancellation		
	Connector	RJ45		
	Electrical	Unconditioned 19-26 AWG twisted pair		
	Sealing current	Max. 20mA source current		
	Clock Source	From System, Line		
	Diagnostic Test	G.SHDSL Loopback :To-LINE, To-bus		
	(vii) TDM over Ethernet Card			
	Combo Gigabit Ethernet (GbE) Interface	(i) Number of Ports 2 (ii) Speed 10/100/1000M bps (iii) Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection		
	Gigabit Ethernet (GbE) Interface	(i) Number of Port 2 (ii) Speed 10/100/1000 Base T (iii) Connector RJ45		
	Ethernet Function	MDI/MDIX for10/100/1000M Base T auto-sensing Ping function contained ARP Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)		
	(vii) Basic Features: (viii)			
	Packet Transparency	Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad(Q-in-Q)		
	QoS	User configurable 802.1p CoS, ToSin Outgoing IP frame		
	Traffic Control	(a) Ingress packet Rate limiting buckets per port for Ethernet port (b) Supporting Rate-based and Priority-based rate limiting for LAN port. (c) Pause frame issue when the traffic exceeding the limited rate before packet		

		dropped following IEEE 802.3X		
	Link Aggregation	WAN support link aggregation		
	Jitter & Wander	PPM: As per G.823 Traffic PPB: As per G.823 Synchronous		
	(ix) Standard Compliance			
	IEEE	802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX		
	(x) Co-directional port(interfaces) should comply with the following specifications:-			
	Interface	ITU G.703 64Kbps co-directional interface		
	Connector	120 ohm,RJ48		
	Line Distance	Upto 500 meters		
	Loop back	DTE Payload Loop back, Local Loop back		
	(c) Clock Source	Internal, E1/T1Line, External		
	(d) Alarm Relay	Alarm Relay : max. Voltage 3Vdc/ max. current: 1A Fuse alarm, and performance alarm		
	(e) System Configuration Parameters	Active Configuration, Stored Configuration, and Default Configuration		
	(f) RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH		
	(g) Performance Monitor			
	Separate Registers	Network, user, and remote site		
	Performance Reports	Should be able to generate Reports for Bursty, Severe Errored and Degraded Network connection for seconds and minute basis.		
	(h) Diagnostics			
	Loopback	E1/T1 interface (Line Loopback, Payload Loop back, Local Loop back), DTE Loopback (DTE-to-DTE, DTE to Line)		
	Test Pattern	For Controller : 221-1, 215-1, 211-1, 29-1, and4-bye user define pattern		
	(j) Front Panel			
	LED	1 per V.35-interface, ACO, Power, SYNC/TEST,LOF,BPV,RAI/AIS		
	(k) Physical/Electrical			
	Dimensions	Not to exceed 450x225x225mm(W×H×D)		
	Power	Single/Dual-48VDC :-36to-75VDC,150 Watts max.		
	Temperature	0-55°C		
	Humidity	0-95% RH (non-condensing)		
	Mounting	Desk-topstackable,19" rack mountable		
	Line Power supply	Available only with DC power for G.SHDSL card only		

	Power Consumption	Max 110 Watts		
	(l) The OEM should have authorized R & D & Repair/ Replacement center in India			
	(m) Compliance	ITU G.703, G.704, G.706, G.732, G.736, G.823,G.826,G.711,G.712,G.775,O.151, V.11,V.28,V.54		
	(n) Card Configuration required as part of supply.			
		Controller (CPU) card -1 no		
		48V DC Power Supply Card- 1No		
		3-Port E1 card–1No		
		2-port Router Card–1No		
	(o) DC Power Source (-48V)	(i) Input 230 V AC (Range 170-264 V AC, single phase, 50Hz).		
		(ii) Output Current:- 8Amp		
		(iii) Size : Not more than 500(W) x 400(D) x175(H) mm with screw terminals at front		
		(iv) Should have short circuit protection.		
38.	**Network Time Server**			
	(a) **Power Supply**			
	(i) Voltage - 230 +/- 10% V AC			
	(ii) Frequency - 47-55 Hz			
	(b) **Features/ Functions**			
	(i) Time Facility - Using Universal Time co- ordination (UTC)			
	(ii) Propagation delay Compensation - Supported			
	(iii) Accuracy - +/- 250 Nanosecond			
	(iv) Time Accuracy - Better than 1 PPM			
	(v) LCD Display - Front panel LCD display to show status, time and no. of satellites			
	(c) **Inputs -** GPS Antenna input through BNC connector.			
	(d) **Outputs**			
	(i) NTP output (2 nos. customizable) for NTP client access through RJ-45. Both Ports shall be independent			
	(ii) RS 232 serial port output (2 Nos)			
	(iii) Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).			
	(iv) Support Client request per Second - 10,000			
	(e) **Antenna**			
	(i) Length of GPS - 50 meters			
	(ii) Gain - over 30 DB			

	(f) Receiver, global positioning System, Display type : LCD Display size : 2 x 3.5 inch; Display resolution : 240x400 pixels Data interface : Ethernet PC interface : Ethernet Expansion slot type : USB Way points : 2 Server frequency : 48-55 Hz Operating temperature : 0-55 deg C Electrical rating : 230V AC Additional information : With antenna and surge arrestor		

(Lt Col Smita Bagbande)
SO1 (Comn & IT)
HQ DGAR

(Maj Gen Alok Naresh)
IG AR (S)
HQ DGAR

(Kamlesh Kumar)
Team Commander
NSG

(Dy Comdt Madhvendra Singh)
ITBP

(SI/T Pardeep Kumar)
CRPF

(Asst Comdt Sandesh Kumar)
SSB

(HS Sri Hari)
Dy Director
DCPW

Approved/ Not Approved

30/3/21

(Sukhdeep Sangwan)
Lt Gen
Director General Assam Rifles

COUNTER SIGNATURE

(KULDIEP SINGH)
D.G. CRPF, DTE. GENL.

TRIAL DIRECTIVES

CENTRALISED INVENTORY MANAGEMENT SYSTEM (CIMS)

All parameters/ specifications mentioned in QRs will be checked by the Board of Officers by ascertaining/ verifying following checks in the presence of Vendor/ Supplier/Manufacturer. In case of any discrepancies/ problem, the representative of firm will demonstrate the features to the Board of Officers. Further, if proper testing Instruments for testing these parameters are not available with customer, same will be arranged by the firm:

(i) Physical Check :- In this category, specifications of the equipment will be checked by B.O.O. Physical check as per QRs.

(ii) Functional Check :- In this category, supplier will show practically all features/ configuration to the board of officers during trial.

(iii) Submission of Certificate:- Specifications which cannot be checked due to lack of testing facilities/ expertise, certificate of any Govt lab or NABL/ILAC accredited laboratory be submitted by the firm.

Ser No.	Specifications	Trial Directives
1.	**Requirement Analysis**	
	(a) Centralised Inventory Management System (CIMS) is a turnkey project. The aim of the subject procurement is to have a proper accounting of stores from its procurement to its condemnation and thereafter procurement of its replacement which must have a paperless functioning of the entire inventory management system.	BOO to check it physically.
	(b) Vendor to analyse present system in Assam Rifles and user requirements to arrive at a proposed solution for the system in terms of Software characteristics. The deliverables in this Phase would include (i) Analyse the present system to understand the short comes and thereafter to study user requirements. (ii) Defining the proposed system in detail. (iii) Preparation of implementation plan. (iv) Approval of implementation by HQ DGAR. (v) Revise the plan as required. (vi) Implementation of final plan after due approval from HQ DGAR.	BOO to check it physically.
2.	**High Level Design**	
	(a) The Software presently in being developed only for Signals Communication Equipment. However in future, HLD should have a provision for subsequent expansion to include stores of other branches that deal with Civil Engineering stores, Clothing, Arms/amn, veh & its spare parts, Rations and other war like stores. (b) Vendor will provide the following on approval of implementation plan.	BOO to check it physically.

	(i) Build Functional Data Model (ii) Build Functional Process Model (iii) Define System performance criteria (iv) Define Architectural Standards (v) Build Prototype (c) Prepare Functional Specifications for each Unit (module) Process.	
3.	**Low Level Design**	
	(a) Do the detailed design of the Software components. (b) Write specifications of various software components based on High Level Design. (c) The Function design documentation should allow the user to approve the description of each Unit Process and contain sufficient details to allow the development Team to process with System Construction activities. The Phase includes following activities: (i) Build Physical Data Model (ii) Build Physical Process Model	BOO to check it physically.
4.	**Platform and Database Agnostic**	
	(a) It would also be required that the application provider should be able to deliver application on latest IT Infrastructure & system software components	BOO to check it physically and firm to produce relevant documents.
	available at Data Centre, Laitkor. Vendor would ensure that the application developed can overcome the technology dependencies and be available to a variety of user access the network.	
5.	**Software Engineering Standers**	
	It is important that software engineering standards are adopted during the initial stages of the development lifecycle to ensure that the developed solution is able to meet quality certifications and security testing. Following certification would be produced (a) CMM level 3.0 or better for software devp. (b) Third party evaluation certificate from CERT certified evaluators.	BOO to check it physically.
6.	**Software Development : The Software Developed should have**	
	(a) Platform Multi-level independent design	BOO to check it physically and firm to produce relevant documents.
	(b) AR defined multi-level user privileges and access.	
	(c) Password encryption for access control	
	(d) Multi-user level access of the menu tools and reports	
	(e) Viewing the report in web browser	
	(f) Explorer style data view	
	(g) Exporting old data in a separate archive database	
	(h) Using resource file	
	(j) Dynamically generating Error Log File	
	(k) Separate tools for recovery of the database in case of corruption of the database.	

	(l) MIS report available to selected user only	
	(m) System schedule to perform automatic backup on every day basis.	
	(n) Adequate provision of complete data security.	
7.	**Construction, Compilation and Testing**	
	Produce Unit tested Software components. This include following activities: (a) Program Physical Data Model (b) Program Physical Process Model (c) Prepare User guides and documentation (d) Conduct Unit Testing with demo data.	BOO to check it physically and firm to produce certification.
8.	**Dashboards**	
	(a) As a senior management tool, most senior officers require dashboards to review total holding of stores, its deficiency, serviceability state, service progress, service levels escalations, alerts and reminders, massages etc. (b) As an operational tool it is required by the office staff for work-list detailing, alerts, reminders and messaging. (c) As configurable component, it would ensure that the user is able to see his role based dashboard for summary of tasks and activities to be completed.	BOO to check it physically.
9.	**Training, finalizing implementation.**	
	(a) **Inital Training**. On successful implementation, proper training on all modules will be provided by the vendor as per plan and schedule provided by HQ DGAR. The training will consist of the following : (i) Hands-on Training during implementation. (ii) On successful implementation, first phase of formal training will be provided for 10 working days for persons of Assam Riffles at Shillong. (iii) Package will be handed over in running condition. (iv) Hand – holding during entire warranty period.	BOO to check it physically.
	(b) **Refresher Training**. There will be five refresher trainings after initial training at the gap of six months. The duration of each refresher training will be for 10 working days for persons detailed by HQ DGAR.	BOO to check it physically and firm to produce relevant documents.
10.	**Backup of Data**	
	(a) The complete solution should be installed, available and controlled at/ from DC location ie HQ DGAR. Data access should be available upto Battalion level using Assam Rifles network.	BOO to check it physically and firm to produce relevant documents.
	(b) The complete backup of the system must be available at DR location ie ARTC&S, Sukhovi and regular backup must be updated on daily basis.	
11.	**Documentation**	
	(a) Providing Detailed documentation for managing system technically and at User Level. (b) Documentation to include Technical Documentation & User Manual for the Entire Developed System. (At least one	BOO to check it physically and firm to produce

	hard and one soft copy of the same to be made available to Assam Rifles Signal Unit and HQ DGAR each. (c) The source code of complete solution with all relevant programmes to be handed over to HQ DGAR after successful implementation of the solution.	relevant documents.
12.	**Solution Sizing and Scalability**	
	Since the solution will be required to be hosted on various deployment models, it is important for the solutions to be able to scale up to meet increasing usage requirements. Although an initial estimation of the hardware specification (quantity and model/version) would be required to size the solution based on system interaction, to increase capacities the solution should be adaptable to scaling. The following should be kept in perspective. (a) Solution should be able to handle increasing number of first time users, transactions, data sharing processes etc. (b) Solution should be able to handle increasing number of concurrent users, concurrent transactions, synchronous data sharing with other systems etc. (c) Solution should be able to perform to the agreed service levels regardless of the bandwidth available or in multiple bandwidth availability scenarios. (d) Solution should be easily scalable to other branches even though they have different products in their inventory. (e) Solution should optimally use technical resources such as memory, processor (CPU), storage etc. In addition should optimally use data centre resources on available bandwidths.	BOO to check it physically and firm to produce relevant documents.
13.	**Application design for occasionally connected systems**	
	For the small percentage of functionality that requires "occasional disconnected /offline" operations, applications may be designed to use a local persistent store/cache just for the purposes of offline capability and later sync as and when connectivity is restored.	BOO to check it physically and firm to produce relevant documents.
14.	**Legacy Integration – Digitization & Migration**	
	(a) The solution should provide for manual data entry of legacy data (allow for conduct of digitization activities).	BOO to check it physically and firm to produce relevant documents.
	(b) Solution should support migration legacy data through be-spoke utilities which allow for data entry, extraction and submission of data into the proposed solution.	
15.	**Intellectual Property Rights**	
	(a) The Intellectual property Rights for the developed product will reside with Assam Rifles. This should include the source code, release management artifacts and all other technical and domain related documentation for the developed solution which will be handed over in softcopy to Assam Rifles on completion of project. The licenses procured for the implementation of the existing application will be provided to Assam Rifles. The software developed should not depend on any propriety basic	BOO to check it physically and firm to produce relevant certificates and

	software for which annual license fee is required to be paid by user. Also, any license required during warranty period will be provided by the vendor at his own cost.	documents.
	(b) The IPR for the developed product / solution should not be restricted / compromised through any legal interpretation. The solution should unambiguously be the property of Assam Rifles.	
	(c) The vendor shall provide at his cost everything necessary for the proper execution of the project according to the intent, requirements and Specifications taken together whether the same may or may not be particularly necessary shown or described therein provided that the same can reasonably be inferred there from.	
16.	**Free Issue Materials**	
	(a) All materials or equipments supplied by the Customer for use in the Contract shall be kept by the Contractor strictly for use in the Contract and shall not be re-allocated to any other work whatsoever without the prior consent in writing of the Customer.	BOO to check it physically and firm to produce relevant documents.
	(b) All materials or equipments so supplied shall remain the property of the Customer. The vendor shall at all times and places until completion of the Contract, keep and maintain such material and equipment under proper conditions.	
	(c) The vendor shall be liable for all loss or damage however caused to such material and equipment throughout the whole of the period during with they are in its custody and until return to the Customer.	
17.	**Store Management System**	
	(a) The entire system should be deployed on ARWAN and should be accessible over ARWAN to all locations of AR. The data accessibility has to be optimized for minimum bandwidth consumption using Caching at Local Systems and server side processing.	BOO to check it physically and firm to produce relevant documents.
	(b) The entire system will be deployed centrally through which branch/ HQs/Units can utilize its computing power of their localized system and get the benefits of the Centralized Inventory Management System.	
	(c) The system should store a Centralized Database which is to be used by branch/ HQs/Units as per access rights granted by HQ DGAR	
	(d) The system should have option to create users	
	(e) The system should have different levels of users Admin Level Users & Data Entry Level Users	
	(f) The system should allow different privileges for differen levels of users	
	(g) The system should allow admin level user to access MIS module	
	(h) The system should have option to add/modify/delete units/formations details	
	(j) The system should have option to add/modify/delete branch details	BOO to check it physically and firm to produce relevant
	(k) The system should have option to authenticate users	
	(l) The system should have option to store/ add/ modify/ delete item category details	

	(m) The system should have option to store accounting units for items	documents.
	(n) The system should have option to store Item Master Details	
	(o) The system should have option to store Vendors details	
	(p) The system should have option to add Store details	
	(q) The system should have option to store supply order details.	
	(r) The system should have option to store serial number/ registration number of the item (if available) along with make and model of the store.	
	(s) The system should have option to store items under expendable category.	
	(t) The system should have option to store its life cycle and must indicate the date of condemnation of the equipment based on life cycle.	
	(u) The system should have option to store details of warranty period / AMC details.	
	(v) The system should have option to store its serviceability status and repair status.	
18.	**Receipt of Stores**	
	(a) DRS: - When store will be received, DRS will be prepared	BOO to check it physically.
	(b) Depot Receipt: - If store receipt from depot, firstly DRS will be prepared and then item will be taken charge on RV	
	(c) **Local Purchase**: - When store receipt from firm, DRS will be prepared and item will be taken charge in CRV	
	(d) **Merge Issue**: -	
	(e) In case cancellation required due to non-collection of item or any other reason, then the issue store to be merged with depot stock and taken on charge by means of CRV	
	(f) **Master Date Record**: - Should have record of all the units and option for addition of new unit	
	(g) **Unit Master**: - For adding new unit	
	(h) **Item Master**: - After receipt the new introduced item which are not in the existing inventory add the item	
	(j) **Due Out**: - All the Dues out item wise, unit wise to be added in master record.	
	(k) **Dues In**: - All the item dues in item wise and vendor wise to be added	
	(l) **Vendor**: - Name of all the firms to be included and on receipt of item	
	(m) **Cost and Date of Purchase** :- Cost of each item and date of purchase to be included	
	(n) **Project case file** :- Each item to include project case file number under which it has been procured	
	(o) **Rejected Stores**: -	
	(p) Details of all the rejected stores to be included in the master date record	
19.	**Section**	
	(a) For addition of new section	BOO to check it physically.
	(b) **Depot**: - For addition of new depot	
	(c) **Casting Error Account Card**: -	BOO to check

	(d) When any error in Account Card these option are use	it physically.
	(e) **Annual Stock Taking**: -	
	(f) The stock taking List for annual stock taking should be generated by the package	
	(g) The system should have option to generate issue vouchers for new demand.	
	(h) The system should have option to generate demands for issue to required items	
20.	**Issue of Store**	
	(a) When the unit demand is being controlled the package should reflect the particular item stock, MSP, Dues in, Dues out, criticality of store if stores are available issue stores otherwise dues out to be maintained automatically. In one voucher six item to be printed as well as operator should have flexibility to increase or decrease the item	BOO to check it physically and firm to produce relevant documents.
	(b) When stores are issued against the dues out maintained on receipt of stores, further part voucher to be generated automatically	
	(c) Package should have option for two types of voucher, regular and further part voucher.	
	(d) Issue registration progress sheet (IRPS) should be printed as and when vouchers are generated. The IRPS sheet should be automatically seen at stores shed and traffic computer	
	(e) The system should manage the dues out automatically	
	(f) **Dues out Clear**: - When store receipt from depot or firm store are taken on charge. Package should reflect automatically dues out if any when receipt is taken on charge	
	(g) **Dues out Renew**: - package should prompt as and when renewal of Dues out is required	
	(h) **Dues out Cancel** :- When unit move out of dependency then all dues out item wise are cancelled and cancellation cert is generated which can be taken on electronic media along with soft copy and other units are enable to retrieve Data for issue/ maint dues out against the unit	
	Issue-in-Lieu: - Option to be included in the package	
	(k) **Transfer Unit Dues Out**: - The dues out of station, stores to be automatically transferred to the new incoming unit	
	(l) **Dues Out Upgrade**: - Option for up gradation of dues out quarterly/ Annually to be included	
	(m) The system should be able to carry out review based on the issue/receipt and MSP of all items to be fixed by software application before finalization of Annual Procurement plan	
	(n) The option for accounting of salvage stores to be included manually procedure followed has been studied and requirement noted by the firm reps	
	(o) The system should have option to receive item for repair from units and other branches	
	(p) The system should have option to send items to vendors for repair	
	(q) The system should have option to receive items from vendors after being repaired	
	(r) The system should have option to return item to	

	respective unit after repair	
21.	**Reports Generation**	
	(a) The system should generate stock report of all the items.	BOO to check it physically.
	(b) The system should generate available stock report for the list of items	
	(c) The system should generate report for the list of items issued, date wise, unit wise ,etc.	
	(d) The system should generate notification if the demand is not processed for certain period of time	
	(e) The system should generate report for the list of items received for repair	
	(f) The system should generate report for the list of items given for repair	
	(g) The system should generate report for the list of item received after being repaired	
	(h) The system should generate report to show the list of stores issued.	
	(j) The system should generate report to indicate expiry of warranty / AMC	
	(k) The system should generate report to indicate expiry of life cycle	
	(l) The system should generate report for deficiency of given items as per authorisation of Assam Rifles	
	(a) The system should generate report giving details of unserviceable/ under repair items	
	(b) **Reports to be Printed**	
22.	**Print of Account Card**	
	(a) System should have facility to prepare and print customized report based on any combination of above	BOO to check it physically.
	(b) Print Account card all items	
	(c) Print Account Card only for transaction made	
	(d) Dues out all items particular unit (LCC)	
	(e) Dues out all particular item all units	
	(f) Dues out all items particular unit	
	(g) Dues out particular unit particular item	
	(h) Dues out all items particular unit (expandable)	
	(i) Issue particular item all units	
	(j) Issue particular item particular unit	
	(k) Issue particular unit all items	
	(l) Issue details all items (LCC)	
	(m) Issue details all items (Expandable)	
	(n) Receipt particular item from all depot	
	(o) Receipt from LP of particular item	
	(p) Receipt from all depot particular section	
	(q) Receipt details all item particular period	
23.	**Printing of Maintenance Report**	
	(a) Details of issue per day	
	(b) Details of receipt per day	
	(c) View inventory details	
	(d) Surplus inventory details	
	(e) Deficient inventory details	
	(f) Non-moving items	

24.	**Printing of details of Dues in items from various firms**	BOO to check it physically.
	(a) List of item dues In from firm	
	(b) List of item where delivered period expired	
	(c) More than one year	
	(d) More than six month	
	(e) More than three month	
	(f) Less than three month	BOO to check it physically.
	(g) List of receipted vouchers pending from units for specified period.	
HARDWARE SPECIFICATIONS		
25.	**High End Switch**	
	(a) **Architecture**	
	(i) Modular architecture, minimum four slots for interface modules	BOO to check it physically and firm to produce relevant documents and certifications.
	(ii) Shall have two dedicated management module slots in addition to the interface modules	
	(iii) Shall have CLOS Architecture or equivalent shared (iv) switch fabric capability with minimum four switch fabrics all supporting active switching to support high switching capacity	
	(v) Shall have fully distributed architecture (any additional hardware required for the same shall be proposed before technical evaluation and any changes after that will be provided additionally by vendor at his own cost)	
	(vi) Shall provide distributed Layer-2 (switching) and Layer-3 forwarding (Routing) on all line cards (any additional hardware required for the same shall be proposed before technical evaluation and any changes after that will be provided additionally by vendor at his own cost)	
	(vii) Shall have minimum 3.2 Tbps of switching capacity or higher	
	(viii) Shall have 8 x10 G SFP+, 16 x1 G-SFP and 48x10/100/1000 Base T ports functional from day-1	
	(ix) Shall be 19" Rack Mountable	
	(x) The Switch should have inbuilt/ pre-loaded operating system with modular architecture	
	(b) **Advanced Service Modules support**. The switch shall support service modules to port applications directly to the switch chassis. This shall include support VPN Firewall module	
	(c) **Resiliency**	
	(i) Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 router	
	(ii) Shall support virtual switching fabric creation across four chassis-based switches using 10G Ethernet Links	
	(iii) Should support Virtualizes a physical switch into multiple logical devices, with each logical switch	

	having its own processes, configuration, and administration	
	(iv) Should support Hot-swappable Modules	
	(v) Passive backplane with no active components for increased system reliability	
	(vi) IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol	
	(vii) IEEE 802.3ad Link Aggregation Control Protocol (LACP)	
	(viii) Ring protocol support to provide sub-100 ms recovery for ring Ethernet-based topology	
	(ix) Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments	BOO to check it physically and firm to produce relevant documents and certifications.
	(x) Graceful restart for OSPF, IS-IS and BGP protocols	
	(xi) Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP protocols	
	(x) The Switch support In-Service Software Upgrade (ISSU)	
	(d) **Layer 2 Features**	
	(i) Shall support up to 4,000 port or IEEE 802.1Q-based VLANs	BOO to check it physically and firm to produce relevant documents and certifications.
	(ii) Shall support GARP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs	
	(iii) Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops	
	(iv) Shall support IEEE 802.1ad QinQ and Selective QinQ to increase the scalability of an Ethernet network by providing a hierarchical structure	
	(v) Shall support Jumbo frames on GbE and 10-GbE ports	
	(vi) Internet Group Management Protocol (IGMP)	
	(vii) Multicast Listener Discovery (MLD) snooping	
	(viii) IEEE 802.1AB Link Layer Discovery Protocol (LLDP)	
	(ix) Multicast VLAN to allow multiple VLANs to receive the same IPv4 multicast traffic	
	(e) **Layer 3 Features (any additional licenses required shall be included)**	
	(i) Static Routing for IPv4	
	(ii) RIP for IPv4 (RIPv1/v2)	
	(iii) OSPF for IPv4 (OSPFv2)	
	(iv) IS-IS for IPv4	
	(v) Border Gateway Protocol 4 with support for IPv4 addressing	
	(vi) Policy-based routing	
	(vii) Unicast Reverse Path Forwarding (uRPF)	
	(viii) IPv4 tunneling to allow IPv4 packets	
	(ix) Dynamic Host Configuration Protocol (DHCP)	

		client, Relay and server	
		(x) PIM Dense Mode (PIM-DM), Sparse Mode (PIM-SM), and Source-Specific Mode (PIM-SSM) for IPv4 multicast applications	
		(xi) MPLS and VPLS Support	
		(xii) Should support PBR, OSPF, BGP, NSF, MPLS, VPLS from day one	
		(xiii) Should support Virtual Extensible LAN (VXLAN) with the help of additional line card	
	(f)	**QoS and Security Features**	
		(i) Access Control Lists for both IPv4 for filtering traffic to prevent unauthorized users from accessing the network	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) Port-basedrate limiting and access control list (ACL) based rate limiting	
		(iii) Congestion avoidance using Weighted Random Early Detection (WRED)	
		(iv) Powerful QoS feature supporting strict priority (SP) queuing, weighted round robin (WRR) and weighted fair queuing (WFQ)	BOO to check it physically and firm to produce relevant documents and certifications.
		(v) IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port	
		(vi) Media access control (MAC) authentication to provide simple authentication based on a user's MAC address	
		(v) Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers	
		(vi) Port security and port isolation	
	(g)	**Management Features**	
		(i) Configuration through the CLI, console, Telnet, SSH and Web Management	
		(ii) SNMPv1, v2, and v3 and Remote monitoring (RMON) support	
		(iii) sFlow (RFC 3176) or equivalent for traffic analysis	
		(iv) Management security through multiple privilege levels with password protection	
		(v) FTP, TFTP, and SFTP support	
		(vi) Port mirroring to duplicate port traffic (ingress and egress) to a local or remote monitoring port. Shall support minimum four mirroring groups	
		(vii) RADIUS/TACACS+ for switch security access administration	
		(viii) Network Time Protocol (NTP) or equivalent support	
		(ix) Shall have Ethernet OAM (IEEE 802.3ah) management capability	
	(h)	**Environmental Features**	
		(i) Shall provide support for RoHS and WEEE regulations	
		(ii) Shall be capable of supporting both AC and DC Power inputs	
		(iii) Operating temperature of 0°C to 45°C	

		(iv) Safety and Emission standards including UL ~~60950-1~~; IEC ~~60950-1~~; VCCI ~~Class A~~; EN ~~55022 Class~~ A	
	(j)	**Software Defined Networking (SDN) Capability**	
		(i) The Switch should have Open Flow Open flow 1.3.1 protocol capability to enable software-defined networking from Day one	
		(ii) The Switch should Allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Open flow protocol	
26.	**Unified Threat Management**		
	(a)	**General Requirements**	
		(i) Network security appliance should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) The proposed vendor must have a track record of continuous improvement in threat detection (IPS) and must have successfully completed NSS Labs' (or equivalent) (NGFW Methodology v7.0 testing with a minimum exploit blocking rate of 99%	
		(iii) OEM should be in Leaders quadrant of Gartner's – in Enterprise Firewall Magic Quadrant (or equivalent) as per the latest report	BOO to check it physically and firm to produce relevant documents and certifications.
		(iv) Appliance shall be ICSA certified for Firewall, IPS, Gateway Anti Virus, IPSec VPN, SSL VPN functionalities	
	(b)	**Hardware & Interface requirements**	
		(i) 14 x 1GE RJ45 inbuilt interfaces, 4 x 1GE SFP interface slots from day one	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) The Appliance should have 1x USB, 1x dedicated Console Port	
	(c)	**Performance and Availability**	
		(i) The Firewall should be on ASIC Based multiprocessor architecture with minimum 18 Gbps of Firewall throughput for 1518 byte packet size, 2,000,000 concurrent sessions, and 130,000 new sessions per second support from day one and Firewall Latency should not be more than 3µs	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) Minimum IPS throughput of 5500 Mbps from day one	
		(iii) Proposed solution must support minimum 1 Gbps of SSL Inspection throughput	
		(iv) IPSec VPN throughput: minimum 8 Gbps	
		(v) Simultaneous IPSec VPN tunnels: 500	
		(vi) Should have 200 SSL VPN peer support from d ay one	
		(vii) Proposed solution must support minimum 10 virtual firewall from day one	
	(d)	**Routing Protocols**	

		(i) Static Routing	
		(ii) Policy Based Routing	
		(iii) The Firewall should support dynamic routing protocol like RIP, OSPF, BGP, ISIS	
	(e)	**Firewall Features**	
		(i) Firewall should provide application inspection for LDAP, SIP, H.323, SNMP, FTP,SMTP, HTTP, DNS, I CMP, DHCP, RPC,SNMP, IMAP, NFS etc	
		(ii) IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP	
		(iii) Allows secure deployment of next-generation IPv6 networks, as well as hybrid environments that require simultaneous, dual stack support of IPv4 and IPv6	
		(iv) The firewall should support transparent (Layer 2) firewall or routed (Layer 3) firewall Operation	
		(v) The Firewall should support ISP link load balancing.	
		(vi) Firewall should support link aggregation functionality to group multiple ports as single port.	
		(vii) Firewall should support minimum VLANS 2048	
		(viii) Firewall should support static NAT, policy based NAT and PAT	
		(ix) Firewall should support IPSec data encryption	
		(x) It should support the IPSec VPN for both site-site and remote access VPN	
		(xi) Firewall should support IPSec NAT traversal.	
		(xii) Support for standard access lists and extended access lists to provide supervision and control	
		(xiii) Control SNMP access through the use of SNMP and MD5 authentication.	
		(xiv) Firewall system should support virtual tunnel interfaces to provision route-based IPSec VPN	BOO to check it physically and firm to produce relevant documents and certifications.
		(xv) The Firewall should have integrated solution for SSL VPN	
		(xvi) Should support LDAP, RADIUS, Windows AD, PKI based Authentication & should have integrated 2-Factor Authentication server support & this two factor authentication can be used for VPN users for accessing internal network from outside and for Local users accessing internet from inside the network and for administrative access to the appliance or all of them	
		(xvii) The solution should have basic server load balancing functionality as an inbuilt feature	
		(xviii) Licensing should be a per device and not user or IP based (should support unlimited users)	
	(f)	**Integrated IPS Features Set**	
		(i) IPS should have DDoS and DoS anomaly detection and protection mechanism with threshold configuration.	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) Support SYN detection and protection for both targets and IPS devices.	

		(iii) The device shall allow administrators to create Custom IPS signatures	
		(iv) Should have a built-in Signature and Anomaly based IPS engine on the same unit	
		(v) Signature based detection using real time updated database & should have minimum 10000+ IPS signature database from day one	
		(vi) Supports automatic security updates directly over the internet. (ie no dependency of any intermediate device)	
		(vii) Signature updates do not require reboot of the unit.	
		(viii) Configurable IPS filters to selectively implement signatures based on severity, target (client/server) and operating systems	
		(ix) IPS Actions: Default, monitor, block, reset, or quarantine	
		(x) Should support packet capture option	
		(xi) IP(s) exemption from specified IPS signatures	
		(xii) Should support IDS sniffer mode	
	(g)	**AntiVirus & AntiBot**	
		(i) Firewall should support antimalware capabilities , including antivirus, botnet traffic filter and antispyware	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) Solution should be able to detect and prevent unique communication patterns used by BOTs i.e. information about botnet family	
		(iii) Solution should be able to block traffic between infected host and remote operator and not to legitimate destination	
		(iv) Should have antivirus protection for protocols like HTTP, HTTPS, IMAPS, POP3S, SMTPS protocols etc.	
		(v) Solution should have an option of packet capture for further analysis of the incident	
		(vi) Solution should uncover threats hidden in SSL links and communications	
		(vii) The AV should scan files that are passing on CIFS protocol	
		(viii) The proposed system shall provide ability to allow, block attachments or downloads according to file extensions and/or file types	BOO to check it physically and firm to produce relevant documents and certifications.
		(ix) The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
	(h)	**Other support**	
		(i) Should suport features like Web- Filtering, Application-Control & Gateway level DLP from day one	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) The proposed system should have integrated Enterprise-class Web Content Filtering solution with database which should support over 250 million web pages in 72+ categories and 68+ languages without external solution, devices or hardware modules.	

		(iii) Should support detection over 3,000+ applications in multiple Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)	
		(iv) The product must supports Layer-7 based UTM/Firewall virtualization, and all UTM features should be supported in each virtual firewall like Threat Prevention, IPS, Web filter, Application Control, content filtering etc.	
		(v) The solution should have the flexibility to write security policies based on IP Address & User Name & Endpoint Operating System	
		(vi) QoS features like traffic prioritization, differentiated services,. Should support for QoS features for defining the QoS policies.	
		(vii) It should support the VOIP traffic filtering	
		(viii) Appliance should have identity awareness capabilities	
		(ix) The firewall must support Active-Active as well as Active-Passive redundancy.	
		(x) Solution must support VRRP clustering protocol.	
	(j)	**Management & Reporting functionality**	
		(i) Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI.	
		(ii) Support accessible through variety of methods, including console port, Telnet, and SSHv2	
		(iii) Support for both SNMPv2 and SNMPv2c, providing in-depth visibility into the status of appliances.	
		(iv) Should have capability to import configuration and software files for rapid provisioning and deployment using Trivial File Transfer Protocol (TFTP), HTTP, HTTPS	
		(v) The Firewall applaince should have minimum 450GB of internal storage for local reporting	
		(vi) Solution must allow administrator to choose to login in read only or read-write mode	
27.	**Hyper Convergent Infrastructure**		
	Hyper-Converged Solution for Cloud		
	(a) **Analyst Ratings** The bidder shall propose Hyper Converged Integrated System from vendors placed in the leader's quadrant in the Gartner Magic Quadrant (or equivalent)report.		
	(b)	**HARDWARE AND PERFORMANCE REQUIREMENTS**	
	(i) Offered Hyper-Converged Capacity	The offered appliance shall be based on modular building blocks of up to one computer node. Each block shall be built using a 2U modular chassis / enclosure housing the compute with respective storage capacity. Each of the Server nodes should be individually serviceable, without shutting down the other Server nodes	BOO to check it physically and firm to produce relevant documents and certifications.

	(ii) Hardware Support	Solution must be x86 infrastructure agnostic and available to be deployed on a choice of atleast 3 server OEMs	
	(iii) Hyper-Converged Infrastructure	Proposed solution must be based on converged IT infrastructure platform that integrates storage, compute, networking, hypervisor, real-time deduplication, compression, and optimization along with powerful data management, data protection, and disaster recovery capabilities in a standard x86 server building block.	
	(iv) Functionality	Proposed hardware must be capable to Deduplicate, Compress & Optimize ALL data inline, in real-time, across all storage tiers: All handled with fine data granularity of 8KB data blocks	
	(v) Hardware Specifications	Each Compute Block must come with the following specifications: Dual Intel Intel® Xeon® Gold 5120 Processor or higher Use of All SSD Drives for Caching and Persistent storage. Minimum 5*1.92TB SSD for data storage Minimum 256GB of DDR4 RAM at 2400 Mhz or above 2*40GbE NIC	
	(vi) Resiliency	Proposed solution must be able to support multiple points of failure with no loss of function or data.	
		During a single component failure (of any type) production services are not affected / degraded in anyway	
		Solution will be deployed as a stretched cluster with Zero RTO. Solution should support stretched cluster deployment in a near site metro DC deployment.	
		Each node should have dedicated non-shared dual-PSU's and should be able to sustain single power supply failure. Solution should not utilize micro-server architecture with shared PSU's and other components.	
		Must be able to sustain minimum of simultaneous 2-HDDs failures per node without DU/DL	
		Must be able to sustain minimum of simultaneous 1-HDDs failures in each node of a cluster and across all nodes in the cluster without DU/DL	
		Must be able to sustain one node failure in the cluster. Must be able to sustain 1 NIC port failure	
	(c) SOFTWARE AND FUNCTIONALITY REQUIREMENTS		

	(i) Common Features Included	The proposed solution must be able to provide enhanced functionality by including the following available without compromise in function or performance in both Hybrid as well as All Flash Nodes:	BOO to check it physically and firm to produce relevant documents and certifications.
		Global dedupe, compression and optimization with minimum impact to production workloads and guaranteed CPU and RAM available to user applications	
		VM-centric policy-based backup/recovery/DR	
		WAN-optimized data protection for VM mobility	
		Unlimited real time data Deduplication Function - licenses Included	
		Unlimited real-time data Compression Function -licenses Included	
		Unlimited capacity Backup Function-Included	
		Should include licenses for multi-site deployments of atleast 3 sites	
	(ii) Global Unified Management	Proposed solution must be able to support the following Global Unified Management features	BOO to check it physically and firm to produce relevant documents and certifications.
		VM-centric management through a single pane of glass via the virtualization manager	
		Programmatic interface to enable automated tasks like failover / failback	
		The ability for a single administrator to manage all aspects of the Hyper-convergence from within the Virtualization Manager for all sites	
		Leverage existing investment of servers for hosting VMs and applications while taking advantage of the functionality of the solution	
		Globally manage Backup Policies per Datastore or per VM	
	(iii) VM-Centricity and Mobility	Proposed solution must be able to support the following VM-Centricity and Mobility feature	BOO to check it physically and firm to produce relevant documents and certifications.
		Backups for specific VMs	
		Ability to Move specific VMs between datacenters	
		Cloning specific VMs	
		VM-level backup instead of forcing protection at the datastore or protection domain level	
	(iv) Data Protection	Proposed solution must be able to support the following Data Protection features	BOO to check it physically and firm to produce
		Backup functionality as a feature instead of a separate server / software license	

		Backup must be an independent copy of source Virtual Server and must allow restore of deleted or corrupted source Virtual Server	relevant documents and certifications.
		Backup to disk functionality as a feature instead of a separate license or appliance	BOO to check it physically and firm to produce relevant documents and certifications.
		Replication across separate datacenter as a feature instead of a separate server / software license.	
		Replication across separate datacenters should be optimized with minimum additional overheads. Data should not need to be rehydrated before being transferred to target datacenter.	
		The ability to carry simultaneous out bi-directional replication between two data centers	
		The ability to replicate Any-to-Any in a Mesh Data Center deployment of more than 3 DC's	
		The ability to define backup policy per datastore, a group of VMs or specific VM	
		Data Protection should have RPO of 10 minutes for local backups	
		The ability to execute backup tasks during office hours without impacting to production workloads	
		Data loss protection against a minimum of 2 simultaneous local hard disks failures per node	
		Data loss protection against a minimum of 1 simultaneous local hard disc failures in all nodes of the cluster	
		Data loss protection against single node failure in cluster	
		The proposed solution must be able to provide backup reports for audit purpose	
	(v) Data Recovery	Proposed solution must be able to support the following Data Recovery features	BOO to check it physically and firm to produce relevant documents and certifications.
		Data recovery should be indepent of source Virtual Server	
		Solution should provide a backup catalog to allow any Virtual Server to be recovered to any specific point-in-time	
		Data recovery process should be simple with an RTO in minutes	
	(vi) Disaster Recovery	Proposed solution must be able to support the following Disaster Recovery features	BOO to check it physically and firm to produce relevant documents and certifications.
		The solution must provide a simple failover operation	
		The solution must allow creation of a Runbook to automate recovery of Virtual Servers	
		The solution must allow changing of IP address of recovered Virtual Servers to match target datacenter	

		The solution should allow changing Virtual Server settings (example vCPU, vRAM, VMSwitch) if required	
		The solution must allow the option to test DR failover to separate network with no impact to production workloads	
		The solution should have feature to assist in failback process to Primary datacenter	
	(vii) Private Cloud License	The Proposed solution must be offered with cloud-ready operating system that is ideal for highly virtualized and software defined datacenter environments.	BOO to check it physically and firm to produce relevant documents and certifications.
		It must include Shielded Virtual Machines, software defined networking, Storage Spaces Direct, and Storage Replica; customers receive rights to unlimited Operating System Environments (OSEs)	
		The proposed solution must provide following features: Computing environment: The virtual machine includes the same basic parts as a physical computer, such as memory, processor, storage, and networking. Disaster recovery and backup, Optimization.	
		Solution must have features such as live migration, storage migration, and import/export to move or distribute a virtual machine.	
		It must offer a remote connection tool for use with both Windows and Linux.	
		The solution should have Secure boot and shielded virtual machines that protects against malware and other unauthorized access to a virtual machine and its data.	
		The solution must give virtual machine direct and exclusive access to some PCIe hardware devices. Using a device in this way bypasses the virtualization stack, which results in faster access.	
		The solution must prevent a virtual machine's excessive activity from degrading the performance of the host or other virtual machines.	
		A virtual machine can be used as a host and create virtual machines within that virtualized host.	
		The solution must have option to set up Remote direct memory access (RDMA) on network adapters bound to a virtual switch, regardless of whether switch embedded teaming (SET) is also used.	
		The solution must have features to make it harder for virtualisation administrators and malware on the host to inspect, tamper with, or steal data from the state of a shielded virtual machine.	

28.	**Authentication Tokens**		
	(a) Certification	FIPS 140-2 Level 2 or as per CCA Guidelines CC / EAL 4+	BOO to check it physically and firm to produce relevant documents and certifications.
	(b) Asymmetric Key Operations	• PKCS#11 compliant • RSA signature: 2048 bit or higher • Secure hash: MD5, SHA -1, SHA-256, SHA -512 □ ECC P-Curves	
	(c) Memory	64 KB or more	
	(d) Credential Storage	• X.509 V3 certificates, • secure symmetric key storage • Microsoft Windows Credentials	BOO to check it physically and firm to produce relevant documents and certifications.
	(e) Platform Support	Windows7, 10, Windows Server 2012and higher server OS, Linux OS	
	(f) Random Number Generator	ANSI X9.31 PRNG or NIST DRBG SP 800 90 CTR mode	
	(g) Data Transfer rate	125 Kbps or more	
29.	**Barcode Printer**		
	(a) Printer Type	Direct Thermal / Thermal Transfer	BOO to check it physically and firm to produce relevant documents and certifications.
	(b) Processor & (c) Memory	400 Mhz Processor,	
		min 128 MB Flash, 128 MB SDRAM (standard)	
	(d) Print Methods	Direct thermal and thermal transfer, Printing of barcodes, text and graphics.	
	(e) Resolution	203 dpi/8 dots per mm	
	(f) Print Width	min 4.09"	
	(g) Print Length	min 155"	
	(h) Print Speed	min 6IPS	
	(j) Weight & dimension	not more than 12KG	
	(k) Media handling	6.0" (152 mm) O.D. on a 1" (25 mm) I.D. core	
	(l) Sensors	transmissive sensors & reflective sensor	
	(m) Drivers	linux, Windows 10, Windows 8, Windows 7, Windows Server 2016, Windows 8.1, Windows Server 2012, Windows Vista (32 & 64Bit)	
	(n) Display	Icon-based LCD multilingual graphical user interface and full function keypad	
	(o) Construction and access	Metallic Frame, Bifold Door fo easy access to media	
	(p) Communication and Interface Capabilities	USB 2.0 & RS232	
	(q) Media Spec	Should support min 450 meters ribbon roll	

	(r) Printing language	Should support ZPL, ZPL II, EPL & EPL2	
	(s) Device management	Should be supported by SOTI & Airwatch	
	(t) Cloud printing	the printer Should be able to connect to the Cloud directly and securely, forwarding data from any port.	
	(u) Media handling	Should Support labels with Gap, Mark in roll form; should support fan fold media	
	(v) Input	100-240 VAC, 50-60 Hz	
	(w) Barcode Support	Should Support all 1D and 2D Symblogies	
	(x) Certification	BIS for printer , Energy Star compliant	
	(y) Service Center	OEM should have an ISO certified service center in India for at least 3+ years	
	(z) OEM	OEM should be present in country as a direct entity for min of 5 years and should have sold a min of 50000 barcode printers in India ia and should have a global turnover of over 500 Million for past 3 years (cash flow positive)	BOO to check it physically and firm to produce relevant documents and certifications.
30.	**Barcode Scanner**		
	(a) Technology	Digital imager 2D Barcode scanner	BOO to check it physically and firm to produce relevant documents and certifications.
	(b) Hands free operation	Scanner should operate in hands free mode when placed on stand. Scanner should auto trigger when a barcode is presented	
	(c) Image Resolution	Min VGA (640 x 480) or better	
	(d) Depth of field	min 11 inch for 20 mil QR code for ease of scanning from stand	
	(e) Symbologies	PDF417, MicroPDF417, Data Matrix, Maxicode, QR Code, MicroQR, Aztec. Supports most 1D and 2D Symbologies.	
	(f) Ambient Light Immunity	Scanner should be able read in bright and low light of 0-105,000 Lux (total dark to Bright sunlight)	
	(g) Reading Precision	>=4 Mil code 128 and min 6.7 ,mil QR Code	
	(h) Pitch	Roll Pitch Yaw 0 - 360° ± 65° or greater ± 60° or greater	
	(j) Minimum Symbol Contrast	min 25% MRD	
	(k) Interface	USB	
	(l) Weight	less than 170gms	
	(m) Indication	Beep (adjustable tone) and Visual indication of Good and bad reads	
	(n) Power	Scanner should be powered by USB port. No separate Adaptors should be needed	
	(o) Operating	0 to 50 degrees Celsius	

	Temperature		
	(p) Storage Temperature	-20 to 70 degrees Celsius	
	(q) Humidity	5% to 95% (non -Condensing)	
	(r) Drop & Tumble	should withstand 1.5 meter drop and min 250 tumbles	
	(s) IP Sealing	Min IP42 or above	
	(t) OEM	OEM should be present in country as a direct entity for min of 5 years and should have sold min of 100000 barcode scanners within India and should have a global turnover of over 500 Million for past 3 years (cash flow positive)	
	(u) Warranty	OEM certified 5 (Five) Years onsite 100% comprehensive warranty from Go Live date of Project	
	(v) OEM service centre	OEM should have an ISO certified service centre with in the country operational for min 3 years prior to the tender date	
	(w) Certification	BIS certified	Certificate to be checked
31.	**Application Load Balancer (Architecture)**		
	(a) Should be high performance purpose built hardware with multicore CPU support.		BOO to check it physically and firm to produce relevant documents and certifications.
	(b) The appliance should have 8 GB RAM and 5 Gbps of system throughput to support multiple load balancing features and functions		
	(c) The appliance should have minimum 4 triple speed 10/100/1000 Mbps Gigabit copper ports & option for 2 * 10G SFP+ ports		
	(d) Solid state drive (SSD) for high I/O performance and dual power supply support		
	(e) Hardware based SSL acceleration with 2Gbps of bulk SSL throughput and 2800 2k SSL transactions per second (TPS)		
	(f) USB based fast failover support for automated configuration synchronization and improved failover time as compare to traditional cluster		
	(g) In order to meet high performance requirements load balancer must support virtual grouping (not clustering) of the appliances and must appear as single system.		
	(h) Multiple appliances in virtual group/domain should allow administrator to configure one or more applications application (virtual services) across both physical appliances to meet high performance requirement		
32.	**Load balancing features**		
	(a) Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support		
	(b) The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID,		

	hash header etc.	
	(c) Should support Multi-level virtual service policy routing – Static, default and backup policies for intelligent traffic distribution to backend servers	
	(d) Support for policy nesting at layer 7 and layer 4, solution should able to combine layer 4 and layer 7 policies to address the complex application integration.	
	(e) Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support e-Policies to customize new features in addition to existing feature/functions of load balancer	
	(f) Traffic load balancing using e-Policies should support algorithms including round robin, least connections, shortest response, persistence IP, hash IP, hash IP and port, consistent hash IP and SNMP	
	(g) Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.	
	(h) Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.	
	(j) Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.	
	(k) should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers	
	(l) Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	
	(m) Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.	BOO to check it physically and firm to produce relevant documents and certifications.
	(n) Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation	
	(o) The appliance should support Certificate format as "Open SSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".	
	(p) Should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.	
	(q) Should provide full IPv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for IPv6 phase-2 certification.	
	(r) IPv6 gateway should provide compressive support for IPv6 functions to help with IPv4-to- IPv6 transition without	

	business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT	
	(s) Should support various deployment modes for seamless integration including reverse proxy (IPv6 to IPv4, IPv4 to IPv6) and IPv6 to IPv6 transparent and reverse proxy mode.	
33.	**Network and application security**	
	(a) Should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.	
	(b) Appliance should have security features like reverse proxy firewall, Syn-flood and dos attack protection features from the day of installation.	
	(c) Should support integrated network based firewall to protect against network based attacks; administrator should able to configure the security policies on per interface basis.	
	(d) Proposed solution provide integrated WAF functionality to protect against layer 7 attacks and should support deep packet inspection of HTTP & HTTPS traffic in reverse proxy mode	
	(e) Application firewall should support built in rules to counter application attack, provision should be there to customize predefined application security rules. Should support all kind of attacks including OWASP top 10	
	(f) WAF module should support both detection and prevention mode and policies should be enforced on per virtual services.	
34.	**Clustering and failover**	
	(a) Should provide comprehensive and reliable support for high availability with Active-active & active standby unit redundancy mode. Should support USB based fast failover.	
	(b) should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization, system memory, process health check and gateway health check to support the failover in complex application environment	
	(c) Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway	
	(d) Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.	BOO to check it physically and firm to produce relevant documents and certifications.
	(e) should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to minimize the failover delay	
	(f) Support for multiple communication links for real-time configuration synchronizations including HA group, gateway health check, decision rules, SSF sessions etc and heartbeat information	
	(g) Clustering function should support IPv6 VIP's (virtual service) switchover	
	(h) N+1 clustering support with active-active and active-standby configurations.	
35.	**Centralized management**	
	(a) Centralized management appliance should have extensive reporting and logging with inbuilt TCP dump like tool	BOO to check it physically and

	and log collecting functionality	firm to produce relevant documents and certifications.
	(b) The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.	
	(c) Should support XML-RPC for integration with 3rd party management and monitoring	
36.	**Network Traffic Manager (BANDWIDTH CONTROLLER)**	
	An additional device for bandwidth control should be provided along with the system. The features are as follows.	
	(a) The system should reduce the impact of non-strategic traffic, and diagnose and resolve network problems	BOO to check it physically and firm to produce relevant documents and certifications.
	(b) The system should identify and control bandwidth hogs so that network administrators can identify problem users, applications and websites and apply automated policies to limit or prevent bandwidth allocation.	
	(c) The system should have the feature to easily monitor recreational traffic like video streaming and P2P sharing.	
	(d) **Real-time Monitoring:** The system should monitor the health of network in real time and give insight about how applications are performing, bandwidth consumed by users, applications across the network	
	(e) **Policy-Based Shaping:** The system should have the feature to prioritize how and when users, applications and websites can consume bandwidth on network.	
	(f) **Interactive Analytics:** Intuitive dashboard feature should be there to visualize activities by all users.	
	(g) **Application Acceleration:** The system should support acceleration and caching features.	
	(h) **Predictive Recommendations:** The system should have the feature to study the patterns and trends in the network and automatically make suggestions to repair and improve network performance.	
	(j) **Traffic shaping and Acceleration**	
	(i) Shaping Throughput: - 1 Gbps	BOO to check it physically and firm to produce relevant documents and certifications.
	(ii) Concurrent Flows: - 220,000	
	(iii) Packets per second: - 200,000/s	
	(iv) New Connection Rates: - 10,000/s	
	(v) Acceleration Throughout: - 30 Mbps	
	(vi) Edge Cache Throughput: - 50 Mbps	
	(vii) Optimized Connections: - 6,000	
	(viii) APS Objects 250	
	(ix) SLA Objects 250	
	(x) PDF Reports 60	
	(xi) Traffic Policies 1024	
	(k) **Interface Capability**	
	(i) The system should have 1 x RJ45 based dedicated console port for management purpose.	BOO to check it physically and firm to produce relevant documents and certifications.
	(ii) The system should have at least 3 x 1G (Copper) bypass bridge pair and 2x 1G (Fiber) bypass bridge pair. Also, the system should have one additional NIC slot for future	

	expansion.		
	(I) **Physical Parameters**		
	(i) Form Factor: -1U rack mountable		BOO to check it physically and firm to produce relevant documents and certifications.
	(ii) Power Rating: - 17W @ 0.13A, 22W @ 0.16A (Max)		
	(iii) Environment: - 0 deg C to 40 deg C, 5% to 90% operating humidity.		
37.	**Two units of under mentioned device should provide with the following system.**		
	(a) **SYSTEM PARAMETERS**		
	Speech band	300to 3400Hz	BOO to check it physically and firm to produce relevant documents and certifications.
	Modulation	Pulse Code Modulation	
	No. of channels per system	32 (30 speech channels, 1 terminal Signalingand1Sync.Channel)	
	Sampling frequency	8000 Hz	
	No of sample bits	8 per channel	
	Total bits per frame	256	
	Bit rate	2048 Kbps ± 50ppm	
	Construction and Architecture	Chassis based modular multiplexer Shelf capable of supporting minimum 12 slots for integration of data, voice, fax and LAN traffic	
	Universal Slots	All slots (other than for power and control)should be universal i.e. capable of accepting any type of voice/ data/ fax card manufactured by the same OEM.	
	Add-Drop or Drop - Insert Function	(a) Should be able to add-drop/ drop-insert voice and data at channel (64 kbps) multiple channel (nx64Kbps) and at E1. (b) Add-drop should be software configurable by user in the field	
	Digital Cross Connection function	(a) It should have an inbuilt cross connect facility on the same equipment (b) Cross Connect: It should be able to map the following voice interfaces: (i) E1 to E1 (ii) E&M (two wire or four wire) toe1 and vice versa (iii) FXO/FXS to E1 and vice versa (b) Add-drop should be achievable by software by user in the field	BOO to check it physically and firm to produce relevant documents and certifications
	Redundancy	Dual controller, dual power with load sharing	BOO to check it physically and firm to produce relevant documents and certifications.
	Protection	1 for 1 protection, E1, T1, FOM	
		PDH ring protection, QE1, QT1, FOM, MiniQE1, 3 E1 for DS0SNCP protection	
	Management	Console, Telnet, SNMP, and Inband Management support	

		Craft interface port for connection to external LCD display	
		Compatible to a SNMP based GUI network management system	
	No. of Slots	Should have 16 or more hot plug-in slots with capability to support following cards.	
		Single E1/Quad E1 (G.703)/ Mini-Quad E1/3*E1 card-DS0 SNCP protection	
		X.21/V.35/RS232/EIA530	
		2W/4WE&M	
		QFXO/QFXS/12FXo/12FXS/24FXO/24FXS	
		10/100 Base-T Router Card	
		2/4 channel G.SHDSL card	
		8-channel Dry Contact I/O	
		TDMoE (TDM over Ethernet) with 2 Combo Giga Bit (GbE) interface for IP uplink	
	(b) Interface Support:- The system shall support below mentioned interfaces/Cards.		
	(i) Network Line Interface - E1 should comply with the following specifications:-		BOO to check it physically and firm to produce relevant documents and certifications.
	Number of ports	4 x E1	
	Line Rate	2.048 Mbps ± 50 ppm	
	Line Code	AMI or HDB3	
	Input Signal	ITU G.703	
	Output Signal	ITU G.703	
	Framing	ITU G.704	
	Connector	BNC/RJ48C, DB25S for Mini Quad E1	
	Electrical	120 ohm twisted pair	
	Jitter	ITU G.823	
	(ii) 2*10/100 Ethernet Router Card with capability to handle 64 WANs should comply with the following specifications		
	Number of ports	2 LAN ports, Max. 64 WAN ports, Each WAN port has data rate nx64K bps, 1≤ n ≤32 (≤ 4Mbps for total of all 64WAN ports)	BOO to check it physically and firm to produce relevant documents and certifications
	Physical Interface	10/100 Base Tx2	
	Connector	RJ45	
	Routing protocol	RIP-I, RIP-II, OSPF, Static	
	Supporting Protocols	PPP(IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT, DHCP	
	Diagnostic	Ping, Trace route	
	QoS	Rate limit	
	(iii) 8*10/100 Ethernet Router Card with capability to		

	handle 64 WANs		
	Number of ports	8 LAN ports, Max 64 WAN ports. Each WAN port has data rate nx64K bps.	BOO to check it physically and firm to produce relevant documents and certifications
	Physical Interface	10/100 Base T x8	
	Connector	RJ45	
	Routing protocol	RIP-I, RIP-II, OSPF, Static	
	Supporting Protocols	PPP(IPCP/BCP), MLPPP, HDLC, Frame Relay, and Cisco compatible HDLC, NAT/NAPT,DHCP	
	Diagnostic	Ping, Trace route	
	QoS	Rate limit	
	(iv) Voice Card (8EM) port (interfaces) should comply with the following specifications:-		
	(aa) Connector : RJ45 connector (ab) Alarm conditioning : CGA busy after 2.5 seconds of LOS, LOF (ac) Encoding : A-law or μ-law user selectable together for all. (ad) Impedance : balanced 600 or 900ohms. (ae) Longitudinal rejection: 55dB (af) Loss adjustment : -21 to +10 dB/0.1 dB step transmit and receive (ag) Single/ distortion : >46 dB with 1004Hz, 0 dBm input (ah) Frequency response : -0.25 to -1 dB from 300 to 3400Hz (aj) Signaling : Type1,Type 2, Type3, Type 4, Type5 transmit only		
	(v) Voice card (12FXS/ 12FXO/ 24FXS/ 24FXO) port (interfaces) should comply with the following specifications:-		
	(aa) 12 FXS/ FXO Connector :Twelve RJ11 (ab) 24FXS/FXO Connector : one RJ21X (ac) Alarm conditioning : CGA busy after 2.5 seconds of LOS, LOF (ad) Encoding : A-law or μ-law, user selectable together for all (ae) AC Impedance : balanced 600 or 900 ohms		
	(af) Longitudinal Conversion Loss : >46 DB (ag) Cross talk measure : Max -70 dBm0 (ah) Gain Adjustment: -21 to +10 dB / 0.1dB step transmit & receive (ai) Signal/Distortion : >25 dB with 1004 Hz, 0 dBm input (aj) Frequency Response : -0.25 to -1dB from 300 to 3400Hz, coincide with ITU-TG.712 (ak) Loss adjustment : -21to+10 dB/ 0.1dB step transmit and receive		

	(al) Signal /Distortion: 46 dB with 1004 Hz, 0dBm input (am) Frequency response: -0.25 to -1 dB from 300 to 3400Hz, coincide with ITU-T. (an) Ideal channel noise: Max -65 dBm op (ao) Inter-modulation : coincide with ITU-T B.712 (ap) 2Wire return loss : > 2dB echo, >20 dB signing (aq) FXS loop feed : Nominal -48 V dc with 20 mA Current limit (ar) Signaling : Loop Start, DTMF, pulse, PLAR, Battery Reverse		
	(vi) G.SHDSL Line port (interfaces) should comply with the following specifications:-		
	Number of ports	2 or 4	BOO to check it physically and firm to produce relevant documents and certifications.
	Line Rate for 4 - channel G.SHDSL	nx64 Kbps (n= 3to 31)	
	Line Rate For 2-channel G.SHDSL	nx64 Kbps (n= 3to 15)	
	Line Code	16-TCPAM, full duplex with adaptive echo cancellation	
	Connector	RJ45	
	Electrical	Unconditioned 19-26 AWG twisted pair	
	Sealing current	Max. 20mA source current	
	Clock Source	From System, Line	
	Diagnostic Test	G.SHDSL Loopback :To-LINE, To-bus	
	(vii) TDM over Ethernet Card		
	Combo Gigabit Ethernet (GbE) Interface	(i) Number of Ports 2 (ii) Speed 10/100/1000M bps (iii) Connector RJ45 for twisted pair GbE, LC for optical GbE, auto detection	BOO to check it physically and firm to produce relevant documents and certifications.
	Gigabit Ethernet (GbE) Interface	(i) Number of Port 2 (ii) Speed 10/100/1000 Base T (iii) Connector RJ45	
	Ethernet Function	MDI/MDIX for10/100/1000M Base T auto-sensing Ping function contained ARP Per port, programmable MAC hardware address learn limiting (max. MAC table 8192 (8k) entry)	BOO to check it physically and firm to produce relevant documents and certifications.
	(viii) Basic Features:		
	Packet Transparency	Packet transparency support for all types of packet types including IEEE 802.1q VLAN and 802.1ad(Q-in-Q)	BOO to check it physically and firm to produce relevant documents and certifications.
	QoS	User configurable 802.1p CoS, ToSin Outgoing IP frame	

	Traffic Control	(a) Ingress packet Rate limiting buckets per port for Ethernet port (b) Supporting Rate-based and Priority- based rate limiting for LAN port. (c) Pause frame issue when the traffic exceeding the limited rate before packet dropped following IEEE 802.3X	
	Link Aggregation	WAN support link aggregation	
	Jitter & Wander	PPM: As per G.823 Traffic PPB: As per G.823 Synchronous	
	(ix) Standard Compliance		
	IEEE	802.1q, 802.1p, 802.1d, 802.3, 802.3u, 802.3x, 802.3z, 802.1s, 802.1w, 802.1AX	
	(x) Co-directional port(interfaces) should comply with the following specifications:-		
	Interface	ITU G.703 64Kbps co-directional interface	BOO to check it physically and firm to produce relevant documents and certifications.
	Connector	120 ohm,RJ48	
	Line Distance	Upto 500 meters	
	Loop back	DTE Payload Loop back, Local Loop back	
	(c) Clock Source	Internal, E1/T1Line, External	BOO to check it physically and firm to produce relevant documents and certifications.
	(d) Alarm Relay	Alarm Relay : max. Voltage 3Vdc/ max. current: 1A Fuse alarm, and performance alarm	
	(e) System Configuration Parameters	Active Configuration, Stored Configuration, and Default Configuration	
	(f) RS232 Console Port (VT100)	10 Base-T, Ethernet, SNMP In-band 64 Kbps supports HDLC/PPP, SSH	
	(g) Performance Monitor		
	Separate Registers	Network, user, and remote site	
	Performance Reports	Should be able to generate Reports for Bursty, Severe Errored and Degraded Network connection for seconds and minute basis.	
	(h) Diagnostics		
	Loopback	E1/T1 interface (Line Loopback, Payload Loop back, Local Loop back), DTE Loopback (DTE-to-DTE, DTE to Line)	BOO to check it physically and firm to produce relevant documents and certifications.
	Test Pattern	For Controller : 221-1, 215-1, 211-1, 29-1, and4-bye user define pattern	
	(j) Front Panel		
	LED	1 per V.35-interface, ACO, Power,	

		SYNC/TEST,LOF,BPV,RAI/AIS	
	(k) Physical/Electrical		
	Dimensions	Not to exceed 450x225x225mm(W×H×D)	
	Power	Single/Dual-48VDC :-36to-75VDC,150 Watts max.	
	Temperature	0-55°C	
	Humidity	0-95% RH (non-condensing)	
	Mounting	Desk-topstackable,19" rack mountable	
	Line Power supply	Available only with DC power for G.SHDSL card only	
	Power Consumption	Max 110 Watts	
	(l) The OEM should have authorized R & D & Repair/ Replacement center in India		
	(m) Compliance	ITU G.703, G.704, G.706, G.732, G.736, G.823,G.826,G.711,G.712,G.775,O.151, V.11,V.28,V.54	
	(n) Card Configuration required as part of supply.		
		Controller (CPU) card -1 no	BOO to check it physically and firm to produce relevant documents and certifications.
		48V DC Power Supply Card- 1No	
		3-Port E1 card–1No	
		2-port Router Card–1No	
	(o) DC Power Source (-48V)	(i) Input 230 V AC (Range 170-264 V AC, single phase, 50Hz).	BOO to check it physically and firm to produce relevant documents and certifications.
		(ii) Output Current:- 8Amp	
		(iii) Size : Not more than 500(W) x 400(D) x175(H) mm with screw terminals at front	
		(iv) Should have short circuit protection.	
38.	**Network Time Server**		
	(a) **Power Supply**		BOO to check it physically and firm to produce relevant documents and certifications.
	(i) Voltage - 230 +/- 10% V AC		
	(ii) Frequency - 47-55 Hz		
	(b) **Features/ Functions**		
	(i) Time Facility - Using Universal Time co-ordination (UTC)		
	(ii) Propagation delay Compensation - Supported		
	(iii) Accuracy - +/- 250 Nanosecond		
	(iv) Time Accuracy - Better than 1 PPM		
	(v) LCD Display - Front panel LCD display to show status, time and no. of satellites		
	(c) **Inputs -** GPS Antenna input through BNC connector.		
	(d) **Outputs**		
	(i) NTP output (2 nos. customizable) for NTP client access through RJ-45. Both Ports shall be independent		
	(ii) RS 232 serial port output (2 Nos)		
	(iii) Pulse output: 1 PPS, ½PPM, 1PPM (Configurable).		

	(iv) Support Client request per Second - 10,000	
	(e) **Antenna**	
	(i) Length of GPS - 50 meters	
	(ii) Gain - over 30 DB	
	(f) Receiver, global positioning System, Display type : LCD Display size : 2 x 3.5 inch; Display resolution : 240x400 pixels Data interface : Ethernet PC interface : Ethernet Expansion slot type : USB Way points : 2 Server frequency : 48-55 Hz Operating temperature : 0-55 deg C Electrical rating : 230V AC Additional information : With antenna and surge arrestor	BOO to check it physically and firm to produce relevant documents and certifications.

(Lt Col SmitaBagbande)
SO1 (Comn& IT)
HQ DGAR

(Maj GenAlok Naresh)
IG AR (S)
HQ DGAR

(Kamlesh Kumar)
Team Commander
NSG

(DyComdtMadhvendra Singh)
ITBP

(SI/T Pardeep Kumar)
CRPF

(AsstComdtSandesh Kumar)
SSB

(HS Sri Hari)
Dy Director
DCPW

Approved/ ~~Not Approved~~

30/03/21

(SukhdeepSangwan)
Lt Gen
Director General Assam Rifles

COUNTER SIGNATURE

(KULDIEP SINGH)
D.G. CRPF, DTE. GENL.