

**TENDER SPECIFICATION FOR PROCUREMENT OF
ESTABLISHING DATA CENTERS AND BACKBONE NETWORKING FOR BN
FY 2024-25 / 2025-26**

INTRODUCTION

1. For better understanding and to evaluate all the prospective BIDDERS on same platform, the tender specification has been divided into three parts:
 - a. **Part-1:** General Information and BIDDER'S Responsibility.
 - b. **Part-2:** Operational and Technical Specification.
 - c. **Part-3:** General Terms and Conditions.

2. Prospective BIDDERS are to comply with the requirements and terms & conditions mentioned in Part-1, Part-2, and Part-3 of the tender specification. BIDDERS are also responsible to provide performance/ technical data, brochure, specific figures, layout and information as asked against each condition.

3. Prospective BIDDERS are to submit their offer in two envelopes:
 - a. Technical Offer.
 - b. Financial Offer.

4. BIDDER shall comply all the terms and conditions of the tender documents as compliance statement under the following tabular format:

Tender Article No	Description of Terms and Conditions (as mentioned in Part-1, Part-2 and Part-3 of the Tender)	Compliance/ Remarks by Principal/ manufacturer (To be agreed/ To be mentioned with detail explanations)

Bidder shall comply all the technical requirements stated in the bidder response column in all the ANNEXES. The financial quote is to be submitted separately in local currency, but compliance/remarks are to be indicated in the technical offer.

PART-1: GENERAL INFORMATION AND BIDDER'S RESPONSIBILITY

General Information

5. BN plans to procure **Establishing Data Centers and Backbone Networking as part of Dedicated Secure Network for BN (Quantity: 01 No)**, (hereinafter called as BNNET-P1 in financial years 2024-2025 /2025-2026.

Eligibility of the BIDDER

6. **General Requirements Including Technical Qualifications** BIDDER is to participate in the tender through their enlistment in DGDP in Bangladesh. Eligibility criteria for BIDDER/ manufacturer are as follows:

a. The BIDDER is to be a reputed Manufacturer of Core Network Devices (Core Network Devices means Server, Router, Firewall, manageable switch) of BNNET-P1 having local office in Bangladesh and enlisted in DGDP or enlisted DGDP supplier authorized by the Single Manufacturer of core network devices of BNNET-P1 through authorized channel. At the same time, the bidder have to provide data center devices, cyber security products, passive items and all other components for this turn-key project.

(1) If the BIDDER is a Manufacturer, the BIDDER is to submit an authorization certificate mentioning that they are the original Manufacturer of core network devices (Server, Router, Firewall, manageable switch) and authorized by the manufacturer or authorized distributor / partner of Data Center passive devices (UPS, Chiller, PAC, Generator), Cyber Security devices (Load Balancer, Server Security, End Point Security), passive items (UTP Cable, Fiber Cable) of data centers.

(2) If the BIDDER is not a Manufacturer of core network devices , the BIDDER is to submit Manufacturer's Authorization Certificate (mentioning the tender number) from Manufacturer or authorized distributor/ authorized partner of core network device (Server, Router, Firewall, manageable switch) including assurance of all contractual obligations along with the offer. Moreover, the bidder is to submit the authorization certificate from the manufacturer or authorized distributor/ authorized partner of Data Center passive devices (UPS, Chiller, PAC, Generator),Cyber Security devices (Load Balancer, Server Security, End Point Security), passive items (UTP Cable, Fiber Cable) of data centers (including assurance of all contractual obligations along with the offer).

b. The BIDDER shall have at least 10 (Ten) years working experience on the Information Technology (IT) system and supplied, installed, commissioned, and maintained at least 01 (One) Tier-3 Certified or Tier-3 compliant data center (drawing and designed verified by Uptime Institute,USA or equivalent organization) in Bangladesh. Proof to be submitted with the offer.

c. BIDDER firm shall have valid license/certificate (ISO/IEC 27001: Information Security Management Certified or ISO/IEC 20000: International standard or ISO 9001:2015 for IT service management, to prove their competency and eligibility for the BNNET-P1 project. License/Certificate to be submitted with the offer.

RESTRICTED

- d. BIDDER shall have a valid MOU with a valid license of Internet Service Provider (ISP) - Nationwide Licenses from BTRC of Bangladesh. MOU along with ISP License/Certificate to be submitted with the offer.
- e. The bidder shall have adequate financial backup to support a project of this magnitude. Financial statements for the last three fiscal years, demonstrating adequate financial health of the firm to be submitted with the offer.
- f. The bidder must have key personnel who will lead the project, including project managers, engineers, and technical leads (at least 5 personnel) with relevant experience in Tier-3 certified/standard data center projects. Resumes to be submitted with offer which demonstrate relevant experience in similar projects.
- g. The bidder must have proven experience in implementing redundant systems (N+N or N+1 for power, cooling and network) or and shall have a MOU with a company who have mentioned experience working in Tier-3 or higher Data Center project.

BIDDER's Responsibility

7. **Compliance on Tender.** BIDDER is to comply with all the conditions of this tender specification. The BIDDER is to submit full specifications and relevant documents, latest brochures for the equipment along with the offer. The information in the brochure needs to be self-explanatory and must support and validate the information mentioned in the tender specification. Deviation or variation of information between the brochure and formally offered documents would be treated as non-compliance. BIDDER has to give due attention and compliance on the following:

- a. BIDDER is to provide detailed explanation of the technical matters if deemed necessary and cross-reference to relevant pages of their offer/ original supporting documents.
- b. BIDDER is to provide project schedule, performance/technical data, specific figures, layout and information as asked against each condition of tender specification.
- c. BIDDER is to mention detailed compliance/ non-compliance and their agreement (as applicable) against each condition. DGDP preserves the right to reject those offers which merely mentioned 'Complied/ Agreed' without highlighting required information/ data/ figures/ graphs/layout as asked against each condition.

8. **Export License.** It is the responsibility of the BIDDER to arrange all the export permit/license (Purchaser will provide end user certificate (EUC) if required)for the datacenters and network hardware shall be imported from foreign country.

9. **Clarification on Any Issue.** The BIDDERS may request for clarification on any issue relating to the information contained in the tender specification from NHQ (Directorate of Naval Information Technology - DNIT) in writing with an information copy to DGDP and apply for a clarification meeting at DGDP (if felt necessary) on pre-agreed schedule from DNIT and DGDP.

10. **Pre-bid Meeting.** The BIDDERS are to attend a pre-bid meeting at DGDP within 04 (four) weeks from the day of floating the tender by DGDP. The purpose of the meeting

RESTRICTED

shall be to clarify issues related to the procurement of BNNET-P1. The BIDDER is to forward their queries 10 (ten) days before the pre-bid meeting.

11. **Presentation by BIDDER.** The BIDDER shall be required to give a presentation at BIDDER's expense for any clarification at BN Headquarters as desired by BN any time during evaluation of the offers. In that case, BIDDER is to submit necessary information and bio-data including photographs and passports for foreign nationals (if any) to BN Headquarters (DNIT)-with info copy to DGDP at least 02 weeks before the presentation. The presentation may cover more aspects than those which have been covered in the BIDDER's proposal.

12. **Evaluation Procedure.** The bid proposals submitted by the BIDDERS shall be evaluated primarily on the basis of (but not only) the following elements (not in any priority order). In addition to hard copy, BIDDER is to submit the authenticated soft copy of the compliance sheet:

- a. Eligibility criteria for BIDDER.
- b. Responsiveness and compliance to the Technical Specifications and General Terms & Conditions.
- c. Presentation by the BIDDERS at purchaser designated location.
- d. BIDDER'S submitted certificates.
- e. Financial competitiveness.

13. **Additional Features Offered by the BIDDER.** The BIDDER may suggest and/ or offer features for the system additional to what is described in this tender schedule. In this case, BIDDER has to explain the detailed advantage of that/ those features of the system.

14. **Acceptance/ Rejection of Bid.** DGDP reserves the right to accept or reject any bid or to terminate the bidding process and reject all bids at any time prior to the contract award (without thereby incurring any liability to the BIDDER).

PART-2: OPERATIONAL AND TECHNICAL SPECIFICATION

15. **Name of the Item.** Establishing Data Centers and Backbone Networking.
16. **Quantity.** 01 (One) set.
17. **Name of the PURCHASER.** Directorate General of Defence Purchase for Government of People's Republic of Bangladesh, Ministry of Defence.
18. **Name of the BIDDER.** To be mentioned
19. **Address of the BIDDER.** Address, phone no, email, and website to be provided.
20. **Country of Origin (COO) and Country of Manufacture (COM).**
- a. **Country of Origin (COO).** The country of origin of the offered equipments:
- (1) Network devices are to be from USA/UK/EU/Canada.
 - (2) Passive items (Generator, UPS, Substation equipments, Cooling system, Fire fighting, CCTV are to be from USA/UK/EU/Switzerland/North American/Japan/Turkey/Australia/Malaysia.
 - (3) Ancillary and others utility items from any reputed manufacturer from the above listed country or specially designated country as mentioned in the tender specification.
- b. **Country of Manufacture (COM).**
- (1) Network devices are to be from any country authorized by the OEM where OEM is having there manufacturing plant/ factory.
 - (2) Passive items are to be from any country authorized by the OEM where OEM is having there manufacturing plant/ factory.
 - (3) Ancillary and other utility items from any reputed manufacturer from the specially designated country as mentioned in the tender specification.
21. **Make, Model, Standard and Certification.** The BIDDER is to mention the make and model of their offered products for BNNET-P1. All major items/ equipment/ components are to be manufactured as per the approved international design and Standard. Make, model, and country of origin/ manufacturer of all major equipment are to be mentioned as list given below:

Ser	Scope of Supply	Brand & Model	Manufacturer, Country of Origin
<u>Active Items</u>			
1.	Rack Server	To be mentioned	To be mentioned
2.	Hyper Converge Server	To be mentioned	To be mentioned
3.	Core Router	To be mentioned	To be mentioned
4.	Internet / DMZ Router	To be mentioned	To be mentioned
5.	WAN Router	To be mentioned	To be mentioned
6.	Branch Router	To be mentioned	To be mentioned
7.	WAN Switch	To be mentioned	To be mentioned

RESTRICTED

Ser	Scope of Supply	Brand & Model	Manufacturer, Country of Origin
8.	Distribution Switch	To be mentioned	To be mentioned
9.	FC / SAN Switch	To be mentioned	To be mentioned
10.	Spine Switch	To be mentioned	To be mentioned
11.	Border Switch	To be mentioned	To be mentioned
12.	Service Leaf Switch	To be mentioned	To be mentioned
13.	Leaf Switch	To be mentioned	To be mentioned
14.	SDN Controller	To be mentioned	To be mentioned
15.	POE LAN Switch	To be mentioned	To be mentioned
16.	Industrial Grade Ethernet switch	To be mentioned	To be mentioned
17.	DC-DR Replicator Switch (IPN)	To be mentioned	To be mentioned
18.	Out Of Band Management Switch	To be mentioned	To be mentioned
19.	Distribution switch (L3)	To be mentioned	To be mentioned
20.	Core Firewall	To be mentioned	To be mentioned
21.	WAN Firewall	To be mentioned	To be mentioned
22.	DMZ Firewall	To be mentioned	To be mentioned
23.	Core Firewall 2	To be mentioned	To be mentioned
24.	WAN Firewall 2	To be mentioned	To be mentioned
25.	DMZ Firewall 2	To be mentioned	To be mentioned
26..	Network Access Control	To be mentioned	To be mentioned
27.	Multi Factor Authentication (MFA)	To be mentioned	To be mentioned
28.	DDoS	To be mentioned	To be mentioned
29.	Web Security Appliance (Gateway /Proxy)	To be mentioned	To be mentioned
30.	Email Security	To be mentioned	To be mentioned
Passive Items			
31.	Server Racks with KVM (42U)	To be mentioned	To be mentioned
32.	Rack without KVM	To be mentioned	
33.	Precision Air Conditioning System	To be mentioned	To be mentioned
34.	Automatic Voltage Regulator (AVR), 800 K	To be mentioned	
35.	Generators	To be mentioned	To be mentioned
36.	CCTV System	To be mentioned	To be mentioned
37.	11KV Isolator with vacuum contactor	To be mentioned	To be mentioned
38.	HT Automatic Voltage Regulator (AVR) with Bypass Arrangement	To be mentioned	To be mentioned
39.	11 KV H.T. Switchgear (VCB)	To be mentioned	To be mentioned
40.	Cast Resin Dry Type Transformer	To be mentioned	To be mentioned
41.	Phase Correction Device (PCD)	To be mentioned	To be mentioned
43.	480 KVAR Automatic PFI Plant	To be mentioned	To be mentioned
44.	Rack Automatic Transfer Switch	To be mentioned	To be mentioned

Ser	Scope of Supply	Brand & Model	Manufacturer, Country of Origin
45.	Bus Bar Trunking System(BBT)	To be mentioned	To be mentioned
46.	Access Control System (Reader) (CDC & DRDC)	To be mentioned	To be mentioned
47.	Access Control Reader (Stand Alone) (For UDC)	To be mentioned	
48.	Fire detection and suppression system	To be mentioned	To be mentioned
49.	Main Chiller	To be mentioned	To be mentioned
50.	Workstation (for NOC & SOC)	To be mentioned	To be mentioned
51.	PC (All in one)	To be mentioned	To be mentioned
52.	UPS (Modular)	To be mentioned	To be mentioned
53.	UPS (Stand Alone)	To be mentioned	To be mentioned
54.	Fiber Optic Cable	To be mentioned	To be mentioned
55.	UTP Cable	To be mentioned	To be mentioned

22. **Year of Manufacture.** The Network Hardware (Server, Router, Firewall, Switch, Storage) must be manufactured brand new in 2024 or later. Network Hardware, Server and Storage, and other major equipment, including spares and tools, shall be brand new, with OEM authorized shelf life with a manufacturing date not before 2024. The Network Hardware, Server, Storage and other major equipment should have OEM authorized shelf life at the time of delivery and its service supports should be available for minimum 05 (five) years from the date of acceptance.

23. **Scope of Supply.** The BNNET-P1 shall be an integrated and scalable intranet system for Bangladesh Navy. This system shall have 1 X Central Data Center (CDC), 1 X Disaster Recovery Data Center (DRDC), Unit Data Center (UDC) for Naval bases and ships, Structure Cabling Network, NTTN connectivity between Dhaka-Chattogram-Khulna, Necessary desktop computer for use of intranet, Network Operation Center (NOC), Training and Maintenance activities. The Summary of scope of work are as follows:

a. **Central Data Center (CDC) (Qty-1).** The Tier-III certified CDC shall be supplied in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.

b. **Disaster Recovery Data Center (DRDC) (Qty-1).** The Tier-III standard (Drawing and design vetted by qualified CDCE by supplier) DRDC shall be supplied in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.

c. **Upgradation of NHQ Data Center (Qty-1).** The Tier-II Standard (Drawing and design vetted by qualified CDCE by supplier) NHQ data center shall be supplied by upgrading its capacity in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.

- d. **Unit Data Center (Command HQ) (Qty-11)**. The Tier-I Standard (Drawing and design vetted by project consultant) UDC (Comd HQ) shall be supplied in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.
- e. **Unit Data Center (Base) (Qty-17)**. The Tier-I Standard (Drawing and design vetted by project consultant) UDC (Base) including Cablings and Base network shall be supplied in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.
- f. **Unit Data Center (Ship) (Qty-15)**. The Tier-I Standard (Drawing and design vetted by project consultant) UDC (Ship) including Cablings and Ship's network shall be supplied in compliance with the Standard Specification, including the hardware/equipment, software, works and services as stated in technical specification by the PURCHASER.
- g. **Structure Cabling**. The Bidder supply necessary fiber and UTP cable along with underground, overhead and bulding cabling works services for the structure cabling of the BNNET-P1 as per the requirement of hardware/equipment, works and services as stated in the tender specification.
- h. **Tools and Test Equipment (Package)**. The bidder shall supply necessary tools and test equipment as per the requirement of hardware/equioments/tools as stated in tender specification.
- j. **Spare Parts and Consumables (Optional)**. The BIDDER shall offer the spare parts and consumables as the requirement stated in Tender Specification. If there is any change in part number due to up-gradation of any spare parts and consumables, the BIDDER shall supply the upgraded spare parts and consumables with necessary certificates at the time of delivery.
- k. **Standard Accessories**. Standard Accessories shall be supplied to install and commission the BNNET-P1 system as 'Turn Key' project. The list of standard accessories is to be mentioned in the offer.
- l. **Layout, Documents and Publications**. The bidder is to provide necessary Layout, Documents and Publications (Operator Manual, Maintenance manual, Wiring Diagram, Parts Catalogue) as per the requirement stated in the tender specification.
- m. **Training Package**. The training package (Foreign and Local) shall be provided by the BIDDER in accordance with the requirements as stated in the tender specification.
- n. **Maintenance Support**. The BIDDER shall have to employ a qualified support team at Each site 24/7 during the warranty period as per article 'Maintenance Support During Warranty Period' and Under Annual Maintenance Contract (if selected by purchaser) as mentioned in the tender specification.
- p. **Inspections and Acceptance**. The Factory Acceptance Test (FAT), Post Shipment Inspection (PSI) and Final Acceptance of BNNET-P1 shall be carried out

in accordance with the article '**Inspection and Acceptance**' requirement as mentioned in the tender specification.

q. **Additional Items/ Accessories (If Any).** If any item(s) is not specified but required for the full range operation of BNNET-P1, then the BIDDER shall furnish the list and submit the list with technical offer as "Additional item to be required for BNNET-P1" along with detail technical specification and price to be quoted separately in the financial offer.

r. **Integration with VSAT Link & Tactical Data Link (TDL).** BN VSAT link (Ethernet port) shall work as the backup link of BNNET-P1 Bidder shall provide necessary connectivity from VSAT remote terminal to the data centers. Besides, BN TDL (Ethernet Port) shall also be integrated with BNNET-P1 project. If any item(s) required for those integration and connectivity, then the BIDDER shall mention such item in the technical offer along with price details in financial offer.

s. **Provision for Future Integration.** BNNET-P1 shall have provision to integrate the following ethernet standard network in future.

- (1) Integrational Tactical Radio Link (Bijoy-50) (ethernet Port)
- (2) Integration with IP PABX (Ethernet Port)
- (3) Integration with AFD, Sister Services and BCG (Ethernet Port)

General Features of BNNET-P1

24. **Basic Requirement.**

a. The BNNET-P1 shall be able to fulfil the requirement uninterrupted data (voice, video, data) flow between data centers to end users and capability to run continuously 24/7/365.

b. The BNNET-P1 shall be able to handle cyber threats and protection mechanism for all kind of global and local threats.

c. The BNNET-P1 shall be able to operate in all-weather conditions from all BN Ships and Base uninterruptedly.

d. The BNNET-P1 shall be compatible with the available Armed Forces Network and paramilitary network having similar hardware, software and protocol.

25. **General Features of the BNNET-P1.** The BNNET-P1 system shall have the following design features:

a. **Design Features.** The Data Centers and Networks shall be designed in scalable and modular concept with '**10 Gbe backbone**' between the datacenters (CDC, DRDC and NHQ DC; inside the Datacenter it should be 40 Gbe backbone), '**1 Gbe backbone**' from the datacenters (CDC, DRDC and NHQ DC) to all the UDC/Base/Ship and considering the passive infrastructure of next 15 years of IT growth of BN with expansion capacity upto '**8000 X Workstations/End points**'.

b. **Network Architecture.** Software Defined Architecture (SDN) need to be considered along with Client-Server architecture following the '**Three-layer hierarchical model**' (i.e Core, Distribution, and Access) or internationally implemented any upgraded/higher redundant architecture.

- c. **Control and Authentication.** Server and Client management shall be controlled through '**Active Directory Domain Controller**'.
- d. **Licensing and Subscriptions.** All servers, network devices, firewalls and computer system shall have licensed operating system and security database with updated licensing subscription for '**minimum 2.5 years**' from the date of final acceptance by BN. Licensing shall be verified through OEM web-portal.
- e. **VLAN Support.** VLAN shall be supported upto the access level switch.
- f. **VPN via Public Network.** Authorized Remote Users (outside BNNET-P1) shall have the facility to connect with BNNET-P1 via VPN tunneling through internet backbone.
- g. **Internet Access.** An internet access server shall be installed for software and subscription update service in CDC and DRDC only, which also shall have the provision to access by the limited no of authorized end-user through virtual PC/Proxy server or any other secured means.
- h. **Cyber Security.** The network shall design considering the naval tactical and operational use following the **Zero Trust Architecture** to have maximum security in respect of cyber attack and cyber security. Multi-Factor authentication system and zero trust security models shall be applied. All input-output ports shall be controlled through Active Directory and Network Access Control devices. Workstations shall have end point security. Unit Data center (UDC) shall have layer-4 firewall security and CDC and DRDC shall have Layer-7 firewall security. SSL shall be applied for internal webpage and application to database security. Network IP allocation shall be MAC binder DHCP server.
- j. **Redundancy.** All network devices, servers and software shall have a concurrent backup with a 1:1 redundancy (**active-active**) at Data Center (CDC). DRDC shall have Active-Active or Active-Passive mode as per requirement. Dual redundancy shall be in critical transmission link such as CDC to DRDC, CDC to NHQDC and CDC/DRDC/NHQDC to 11 X UDC (Command HQ).
- k. **Software and Software Update.** All operating system (OS) must be genuine and registered version. CDC shall provide the software update service for the overall network. The network should have the backward compatibility to ensure older version and existing equipments to be able to connect in the BNNET -P1 as well as remote scan should function in a newer version of NMS/ Network software.
- l. **Connecting Media.** High-quality fiber optics (Multi Mode OM4 and Single Mode) and UTP (CAT 6 or higher grade) cable to be used in the network For Ship armored and rugged Cat 6 cable to be used..
- m. **Workstations (Nodes).** All workstation computer shall have the perpetual licensed of latest operating system registered in microsoft portal.

RESTRICTED

n. **Interoperability.** BNNET-P1 System must support integration with existing military systems and technologies using industry standards networking protocols (TCP/IP, Ethernet).

p. **Data Center Building.** Existing office building of BN shall be used for constructing and setting up of data centers at Dhaka and Chattogram. According to the design data of the building, the maximum load taking capacity of each floor is 2.4 KN/m² (22.77 Kg/ft²) as per BNBC. The bidder has to select appropriate equipment/devices/items and must have a plan to distribute the load in the floor so that floor live load does not exceed the loading limit of the floor of the each data centers (CDC/DRC/NHQ DC).

26. **Environmental Condition.** BNNET-P1 shall be all weather capable to operate 24/7/365 in day and night. Due to the hot and humid environment of Bangladesh, all the equipment should be designed to meet the following requirement:

- a. Environmental Temperature: Up to +50°C (Operating temperature to be mentioned)
- b. Relative Humidity: 90% and above (Operating Humidity to be mentioned).
- c. Must be capable for sustained high temp and humid coastal / maritime environment.

TECHNICAL REQUIREMENT AND SPECIFICATION

27. **Technical Requirements of Central Data Center (CDC).** The CDC shall be the central data hub of BNNET-P1. It is to be designed considering the peacetime and wartime security threats, modern trends of cyber security and uninterrupted operation in all weather conditions. The location, important features and parameters shall be considered while designing CDC are explained below:

- a. **Location.** Nou Unit SHAHEENBAG, Dhaka (2nd floor, Multipurpose Utility Building). Space to be used: 9800 sft (2nd Floor), 3500 sft (Ground floor), 2000 sft (outside ground floor).
- b. **Features.** CDC shall be heart of the BNNET-P1. CDC shall have-
 - (1) 30 racks (42U, critical load 5 KW per rack) capacity datacenter with Tier-3 certification (To be certified by Uptime USA or equivalent org) for uninterrupted operation and services.
 - (2) 1 X Network Operating Center (NOC) for monitoring and maintaining the optimum performance of the network.
 - (3) 1 X Security Operation Center (SOC) for identification, investigation and resolve threats and cyber-attacks.
 - (4) Required high performance servers and storage solutions.
 - (5) Meet me room for dealing the interconnectivity issues.
 - (6) 1:1 Hardware redundancy for uninterrupted services.
 - (7) Network backbone of 10/40 Gbps range.

RESTRICTED

- (8) Power distribution with monitored output and automatic switching capabilities.
- (9) Sufficient capacity power supply arrangement to support a minimum of 5 kW power per rack.
- (10) Chiller shade to be constructed with all utility connections by the bidder at ground floor of CDC building. The Generators and Sub-stations shall be installed in the ground floor. The underground oil reserve tank shall be constructed near to the generator installation site. The bidder may collect requirement drawing from End User (DNIT, NHQ). The bidder has to conduct site survey in-details and submit layout along with 3D design with the offer. The cost is to be included in the heading of infrastructure development cost separately.

Note: Floor Layout and relevant information of CDC is to be collected from DNIT, NHQ).

c. **Parameters.**

- (1) Operation Time: 24/7/365 Days
- (2) Cooling system support: 24/7/365 days
- (3) National Power grid Supply Voltage: 415 V, 50 Hz, 3 phase/ 220V, 50 Hz, 1-phase.
- (4) Backup power support: UPS with backup time 30 minutes and Generators with fuel reserved for 03 days.
- (5) Raised floor system with a minimum clearance of 18 inches to allow for proper airflow.

28. **Technical Requirements of Disaster Recovery Data Center (DRDC).** The DRDC shall be the regional HUB and Disaster Recovery Data Center for BNNET-P1. It is to be designed considering the peacetime and wartime security threats, quick shifting mechanism, modern trends of cyber security and uninterrupted operation in all weather conditions. The location, important features and parameters shall be considered while designing DRDC are explained below:

- a. **Location.** NSD, Chattogram (4th floor). Space to be used: 4000 sft (4th Floor), 800 sft (ground space where 2 storied Generator & Substation Shade to be constructed).
- b. **Features.** DRDC shall have-
 - (1) 20 racks (42U, critical load 5 KW per rack capacity datacenter with Tier-3 Standard (To be designed as per Tier-3 datacenter guideline; drawing and design is to be verified and approved by appropriate certification expert/org) for uninterrupted operation and services.
 - (2) 1 X Network Operating Center (NOC) for monitoring and maintaining the optimum performance of the network.
 - (3) Async Replication technology for data.

RESTRICTED

- (4) Meet me room for dealing the interconnectivity issues.
- (5) 1:1 Hardware redundancy for uninterrupted services.
- (6) To be designed with Network backbone of 10/40 Gbps range.
- (7) Power distribution with monitored output and automatic switching capabilities.
- (8) Sufficient capacity to support a minimum of 5 kW per rack.
- (9) Generator and Sub-station shade (800 sft x 2 storied = 1600 sft) to be constructed with all utility connections by the bidder outside the building approx. 700 meters away from data center building. The bidder may collect requirement drawing from End User (DNIT, NHQ). The bidder has to conduct site survey in details and submit layout along with 3D design with the offer. The cost is to be included in the heading of infrastructure development cost separately.
- (10) Chiller to be installed on the rooftop. All cost related to the preparation of rooftop is to be borne by the bidder.

Note: Floor Layout and relevant information of DRDC is to be collected from DNIT, NHQ

c. **Parameters.**

- (1) Operation Time: 24/7/365 Days
- (2) Cooling system support: 24/7/365 days
- (3) National Power grid Supply Voltage: 415 V, 50 Hz, 3 phase/ 220V, 50 Hz, 1-phase.
- (4) Backup power support: UPS with backup time 30 minutes and Generators with fuel reserved for 01 days.
- (5) Raised floor system with a minimum clearance of 18 inches to allow for proper airflow.

29. **Technical Requirement of Upgradation of NHQ Data Center (NHQ DC).** The NHQ-DC shall be the data HUB for NHQ intranet system. It is to be designed considering the peacetime and wartime security threats, modern trends of cyber security and uninterrupted operation. The location, important features and parameters shall be considered while designing NHQ-DC are explained below:

a. **Location.** Navy Headquarter, Dhaka (Floor Layout and relevant information for NHQ DC is to be collected from DNIT, NHQ).

b. **Features.** NHQ Data Center shall have:-

- (1) 8 racks (42U, critical load 5 KW per rack) capacity Tier-2 standard data center (To be designed as per Tier-2 datacenter guideline; drawing and

RESTRICTED

design is to be verified and approved by appropriate certification expert/org) for uninterrupted running.

(2) 1:1 Hardware redundancy (Server, Router and Firewall) for uninterrupted services.

(3) To be design with Network Backbone of 10/40 Gbps range.

c. **Parameters.**

(1) Operation Time: 24/7/365 Days

(2) Cooling system support: 24//7/365 days

(3) National Power grid Supply Voltage: 415V, 50 Hz, 3 phase/ 220V, 50 Hz, 1-phase.

(4) Backup power support: UPS 30 mins.

30. **Technical Requirements of Command HQ (ComdHQ) Network.** The UDC-COMD HQ (Comd HQ Network Room) shall be data HUB Center for the admin authority. It is to be designed considering the peacetime and wartime security threats, modern trends of cyber security and uninrrupted operation. The location, important features and parameters shall be considered while designing UDC-COMDHQ are explained below:

a. **Location.** The location of UDC-COMD HQ (Comd HQ Network Room) are as follows:

- (1) COMDHAKA (+BNS HAJI MOHSIN) at Dhaka.
- (2) COMCHIT (+ provision to link to FB) at Chattogram.
- (3) CSD (+CNRD+IFF Center) at Chattogram.
- (4) COMBAN (+OSTG) at Chattogram.
- (5) COMNAV (+NAVAL AVIATION HANGAR) at Chattogram.
- (6) COMSUB (+SUBMARINE BASE PAKUA) at Pakua.
- (7) COMSWADS (+BNS NIRVIK) at Chattogram
- (8) CHIEF HYDROGRAPHER (+BNHOC + NAIO) at Chattogram
- (9) COMKHUL (+BNS TITUMIR+BNS UPSHAM+provision to Link to FB) at Khulna.
- (10) COMFLOT WEST (+BNS MONGLA+ BN D/Y MONGLA) at Mongla.
- (11) Commandant NATDOC (+BNS SHERE-E-BANGLA) at Patuakhali.

Note: Room and Building layout of Comd HQ network is to be collected from DNIT, NHQ(**if needed**).

b. **Features.** UDC-COMDHQ shall have:-

- (1) 2 racks (42U, critical load 3 KW per rack)) capacity Tier-2 standard (To be designed) Network Room for uninterrupted operation.
- (2) 1:1 Hardware redundancy (Router only) for uninterrupted service
- (3) 1 x Server (NATDOC HQ, COMSUB HQ, COMFLOT West HQ, COMKHUL HQ)
- (4) 1 x Provision for Server, 1 x Router, 1 x Firewall and 1 x Distribution Switch in each UDC-COMDHQ.

RESTRICTED

- (5) To be design with Network Backbone of 10 Gbps range.
- (6) Connectivity to the CDC, NHQDC and DRDC.
- (7) Capability of VoIP Solutions for communication.

c. **Parameters.**

- (1) Operation Time: 24/7/365 Days
- (2) Cooling system support: 24/7/365 days
- (3) National Power grid Supply Voltage: 415 V, 50 Hz, 3 phase/ 220V, 50 Hz, 1-phase.
- (4) Backup power support: UPS 30 mins

31. **Technical Requirement of Base Network.** The UDC-BASE (Base Network Room) shall be HUB for the base network. It is to be designed considering the peacetime and wartime security threats, modern trends of cyber security and uninterrupted operation. The location, important features and parameters shall be considered while designing UDC-BASE are explained below:

a. **List of Base/Unit Network (17)**

- (1) BNS SHEIKH MUJIB at Dhaka.
- (2) RIP MIRPUR at Dhaka
- (3) NAVY HOUSE at Dhaka
- (4) NU PAGLA at Dhaka
- (5) BNS ISSA KHAN at Chattogram.
- (6) BNS ULKA at Chattogram.
- (7) BNS SHAHEED MOAZZAM at Kaptai.
- (8) BNS BHATIARY at Chattogram.
- (9) BNA at Chattogram.
- (10) SMWT at Chattogram.
- (11) BNS PATENGA at Chattogram.
- (12) RIP Chattogram (Sailor's Colony 2).
- (13) BSO/BSD Ctg at Chattogram.
- (14) BN RRB at Chattogram.
- (15) Fwd Base Cox's Bazar
- (16) RIP Khulna
- (17) SOLAM at Khulna

Note: Room and Building layout of Base network is to be collected from DNIT, NHQ (**if needed**).

b. **Features.** UDC-BASE shall have:-

- (1) 1 rack (42U, critical load 3 KW per rack)) Tier-1 standard (To be designed) Network Room for uninterrupted running.
- (2) 1 x Provision for Server, 1 x Router, 1 x Firewall and 1 x Distribution Switch in Network Room
- (3) To be design with hardware grade of 1 Gbps range.
- (4) A network where Internet and Intranet will run parallaly with all the hardware and accessories.

c. **Parameters.**

- (1) Operation Time: 24/7/365 Days
- (2) Cooling system support: 24/7/365 days
- (3) National Power grid Supply Voltage: 415 V, 50 Hz, 3 phase/ 220V, 50 Hz, 1-phase.
- (4) Backup power support: UPS 30 mins

d. **Building Rack and Nodes.** The summary of building rack and nodes for Command HQ and Bases are as follows

(1) **Building Rack.** Connection from Base Network Room to Building Rack using Single Mode Fiber connectivity.

- (a) 1 X 9 U Rack with an expansion facilities upto 2 X 9 U rack, Access Switch (L2 Manageable).
- (b) 1 x Online UPS (3KVA) with generator power outlet.
- (c) 2 x 2 MP Bullet IP Camera.

(2) **Floor Rack.** Building Rack to Floor Rack Multi-mode/Single Mode Fiber connectivity.

- (a) 1 X 6U Rack, Access Switch (L2 Manageable).
- (b) 1 x Online UPS (1KVA) with generator power outlet.
- (c) 2 x 2 MP IP Bullet Camera

(c) **Nodes.** Structure Cabling from BL/FL Rack to each node, dual faceplate RJ-45 (1 for intranet and 1 for internet), 2 X UTP Cable (FL Rack to Nodes).

32. **Technical Requirements of Ship Network (UDC-SHIP).** The UDC-SHIP (Ship's Network Room) shall be HUB for the ship's network. It is to be designed considering the peacetime and wartime security threats, modern trends of cyber security and uninterrupted operation. The location, important features and parameters shall be considered while designing UDC-SHIP are explained below:

a. **Location.** The location of UDC-SHIP are as follows:

- (1) BNS BANGABANDHU (Frigate) at Chattogram.
- (2) BNS SAMUDRA JOY(Frigate) at Chattogram.
- (3) BNS SAMUDRA AVIJAN (Frigate) at Chattogram.
- (4) BNS ABU BAKR (Frigate) at Mongla
- (5) BNS ALI HAIDER (Frigate) at Mongla
- (6) BNS UMAR FAROOQ (Frigate) at Mongla
- (7) BNS ABU UBAIDAH (Frigate) at Mongla
- (8) BNS SHADHINOTA (Corvette) at Chattogram.
- (9) BNS PROTTOY (Corvette) at Chattogram.
- (10) BNS PROTTASHA (Corvette) at Chattogram.
- (11) BNS DHALESHWARI (Corvette) at Chattogram.
- (12) BNS BIJOY (Corvette) at Mongla
- (13) BNS DURJOY(LPC) at Chattogram
- (14) BNS DURGOM (LPC) at Mongla
- (15) BNS ANUSHANDHAN (Survey Sqn) at Chattogram
- (16) Other Ships – With a temporary connection from BNNET-P1

RESTRICTED

Note: Room and Deck layout of Ship's network is to be collected from DNIT, NHQ (if needed).

b. **Features.** Each ship shall have UDC-SHIP as network operation and management center. Ship Network shall:

- (1) 1 rack (15U (depth: 800mm)/25U (depth: 1000mm) (as appropriate) Tier-1 standard (To be designed) Network Room for uninterrupted running.
- (2) 1 x Provision for Server, 1 x Router, 1 x Firewall and 1 x Distribution Switch in Network Room
- (3) Hardware grade of 1 Gbps range.
- (4) Provision for ship to shore connectivity using fiber optics/UTP cable from jetty connection box
- (5) Provision for VSAT connectivity from ships VSAT room using fiber optics/UTP cable.

c. **Parameters.**

- (1) Operation Time: 24/7/365 Days
- (2) Cooling system support: 24/7/365 days
- (3) Ships Supply Voltage: 415 V/ 380 V, 50 Hz/60 Hz, 3 phase/ 220V, 50 Hz/60 Hz, 1-phase. Bidder is to ascertain the requirement during site survey and necessary conversion equipment is to be supplied by the bidder if needed.
- (4) Backup power support: UPS 30 mins

d. **Ship's Rack and Nodes.** The summary of deck rack and nodes are as follows:

- (1) **Ship's Rack.** Connection from UDC-SHIP (Ship's Network Room) to Deck Rack using Fiber connectivity.
 - (a) 2 X 9U/6U (as appropriate) Rack with Distribution Switch (Manageable)
 - (b) 1 X Online UPS (1KVA) rackmount with Ship's Power supply.
- (2) **Deck Rack.** Connection from Deck Rack to Section Rack (Foxl, Maintop and Quarter Deck) using Fiber connectivity.
 - (a) 1 X 6U Rack, Access Switch (L2 Manageable)
 - (b) 1 X UPS line from DK rack or independent.
- (3) **Nodes.** Structure Cabling from SK Rack to each node, dual faceplate RJ-45 (1 for intranet and 1 for internet), 2 X UTP Cable (SK Rack to Nodes).

TECHNICAL SPECIFICATION

Technical Specification of Active Hardware

33. **Active Hardware.** The main data centers (CDC/DRDC/NHQ-DC) and network room (UDC-COMDHQ/UDC-BASE/UDC-SHIP) shall be connected with active devices including servers, routers, switch, firewall and storage as per approved design by the purchaser. The type of active hardware shall be used in the data centers and networks are summarized below along with the short specification:

34. **Active Hardware for CDC.**a. **Servers.**(1) **Rack Server Type-1.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 32 Physical Cores
- (e) RAM Pool : 256 GB
- (f) Storage : Minimum 2.8 TB All flash

(2) **Hyperconverge Server.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 128 Physical Cores
- (e) RAM Pool : 2 TB
- (f) Storage : Minimum 243 TB All flash

b. **Routers.**(1) **Core Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 19 Gbps (SD-WAN mode)
- (d) Port : 4 x 1/10 GE and 8 x 1 GE

(2) **Internet/DMZ Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 90 Gbps (SD-WAN mode)
- (d) Port : 12 x 1/10 GE, 2 x 40 GE & 2 x 40/100 GE

(3) **WAN Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 90 Gbps (SD-WAN mode)
- (d) Port : 12 x 1/10 GE, 2 x 40 GE & 2 x 40/100 GE

c. **Switch.**(1) **WAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.

RESTRICTED

- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(2) **Distribution Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(3) **FC/SAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 1 Tbps
- (d) Port : 32 x 32 Gb SW SFP Ports

(4) **Spine Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 11.5 Tbps
- (c) Port : 28 x 100/40 Gbps, 8 x 400/100 Gbps

(5) **Leaf Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.25 Tbps
- (d) Port : 48 x 1/10/25 Gbps

(6) **SDN Controller.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.

(7) **DC-DR Replicator Switch (IPN).**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.5 Tbps
- (d) Port : 24 x 1/10/25 Gbps

(8) **Out of Band Management Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 170 Gbps
- (d) Port : 48 x 10/100/1000 Base T

(9) **Multi Site Orchrestation System.**

- (a) Brand : To be mentioned.

- (b) Model : To be mentioned.
 (c) Function : Management of multi site SDN Network

d. **Firewall.**

(1) **Core Firewall.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 60 Gbps
 (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(2) **WAN Firewall.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 20 Gbps
 (d) Port : 8 x 10 G and 8 x 1/10G SFP+

(3) **DMZ Firewall.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 20 Gbps
 (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(4) **Core Firewall 2.**

- (a) Brand : To be mentioned
 (b) Model : To be mentioned.
 (c) Throughput : 60 Gbps
 (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(5) **WAN Firewall 2.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 25 Gbps
 (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(6) **DMZ firewall 2.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 25 Gbps
 (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(7) **Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security.**

- (a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 95 Gbps

(d) Port : 8x10/25G SFP+ & 2 x 40/100 G

(8) **Application Delivery Controller (ADC), Web Application Firewall & API Security.**

(a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Throughput : 60 Gbps in L7
 (d) Port : 8x10/25G, 2x 40/100 G SFP+ +

e. **Storage Solution.**

(1) **Storage.**

(a) Brand : To be mentioned.
 (b) Model : To be mentioned.
 (c) Architecture : 02(two) controller update upto 04 controller
 (d) Capacity : 200TB Usable with NVMe hard disk
 (e) Deployment : DC-NDC-DR, sync-sync-async

(2) **Backup Storage.**

(a) Brand : To be mentioned
 (b) Model : To be mentioned.
 (c) Architecture : 02(two) controller
 (d) Capacity : 100TB Usable with SSD hard disk

f. **Security Solution**

(1) **Web Security Appliance (WSA).**

(a) Brand : To be mentioned
 (b) Model : To be mentioned.
 (c) Subscription : 3 Years.
 (d) Function : To provide content filtering capabilities for users who access the internet.
 (e) User : 500

(2) **Network Access Control.**

(a) Brand : To be mentioned
 (b) Model : To be mentioned.
 (c) Subscription : 3 Years.
 (d) Function : To provide content filtering capabilities for users who access the internet.
 (e) User : 500

(3) **Network Detection & Response.**

(a) Brand : To be mentioned
 (b) Model : To be mentioned.
 (c) Subscription : 3 Years.
 (d) Function : A cybersecurity solution that continuously monitors network traffic to identify, detect, and respond to suspicious activities and threats in real-time.

(4) **Deep Discovery Inspection.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 1 Year

(5) **Anti APT Solution (Sandbox).**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.

g. **IP PABX Telephony Solution**

(1) **IPT System.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) IPT Server : 02
- (d) Extension : 200 in Day 1. Upgrade up to 7000
- (e) IP Phone 1 : 140
- (f) IP Phone 2 : 60 (video)
- (g) PSTN Gateway : 02

35. **Active Hardware for DRDC.**

a. **Servers.**

(1) **Rack Server Type-1.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 32 Physical Cores
- (e) RAM Pool : 256 GB
- (f) Storage : Minimum 2.8 TB All flash

(2) **Hyperconverge Server.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 128 Physical Cores
- (e) RAM Pool : 2 TB
- (f) Storage : Minimum 243 TB All flash

b. **Routers.**

(1) **Core Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 19 Gbps (SD-WAN mode)

(d) Port : 4 x 1/10 GE and 8 x 1 GE

(2) **Internet/DMZ Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 90 Gbps (SD-WAN mode)
- (d) Port : 12 x 1/10 GE, 2 x 40 GE & 2 x 40/100 GE

(3) **WAN Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 90 Gbps (SD-WAN mode)
- (d) Port : 12 x 1/10 GE, 2 x 40 GE & 2 x 40/100 GE

c. **Switch.**

(1) **WAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(2) **Distibution Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(3) **FC/SAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 1 Tbps
- (d) Port : 32 x 32 Gb SW SFP Ports

(4) **Spine Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 11.5 Tbps
- (d) Port : 28 x 100/40 Gbps, 8 x 400/100 Gbps

(5) **Leaf Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.25 Tbps
- (d) Port : 48 x 1/10/25 Gbps

(6) **SDN Controller.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.

(7) **DC-DR Replicator Switch (IPN).**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.5 Tbps
- (d) Port : 24 x 1/10/25 Gbps

(8) **Out of Band Management Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 170 Gbps
- (d) Port : 48 x 10/100/1000 Base T

(9) **Multi Site Orchrestation System.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Function : Management of multi site SDN Network

d. **Firewall.**

(1) **Core Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(2) **WAN Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 20 Gbps
- (d) Port : 8 x 10 G and 8 x 1/10G SFP+

(3) **DMZ Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(4) **Core Firewall 2.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.

RESTRICTED

- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(5) **WAN Firewall 2.**

- (a) Brand : To be mentioned (Preferably CheckPoint).
- (b) Model : To be mentioned.
- (c) Throughput : 25 Gbps
- (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(6) **DMZ firewall 2.**

- (a) Brand : To be mentioned (Preferably CheckPoint).
- (b) Model : To be mentioned.
- (c) Throughput : 25 Gbps
- (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(7) **Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security.**

- (a) Brand : To be mentioned (Preferably Cisco).
- (b) Model : To be mentioned.
- (c) Throughput : 95 Gbps
- (d) Port : 8x10/25G SFP+ & 2 x 40/100 G

(8) **Application Delivery Controller (ADC), Web Application Firewall & API Security.**

- (a) Brand : To be mentioned (Preferably Cisco).
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps in L7
- (d) Port : 8x10/25G, 2x 40/100 G SFP+ +

e. **Storage Solution.**

(1) **Storage.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Architecture : 02(two) controller update upto 04 controller
- (d) Capacity : 200TB Usable with NVMe hard disk
- (e) Deployment : DC-NDC-DR, sync-sync-async

(2) **Backup Storage.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Architecture : 02(two) controller
- (d) Capacity : 100TB Usable with SSD hard disk

f. **Security Solution**

(1) **Web Security Appliance (WSA).**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.

RESTRICTED

- (c) Subscription : 3 Years.
- (d) Function : To provide content filtering capabilities for users who access the internet.
- (e) User : 500

(2) **Network Access Control.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : To provide content filtering capabilities for users who access the internet.
- (e) User : 500

(3) **Deep Discovery Inspection.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 1 Year

(4) **Network Detection & Response.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : A cybersecurity solution that continuously monitors network traffic to identify, detect, and respond to suspicious activities and threats in real-time.

(5) **Anti APT Solution (Sandbox).**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.

36. **Active Hardware for NHQ DC.**

a. **Servers.**

(1) **Rack Server Type-1.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 32 Physical Cores
- (e) RAM Pool : 256 GB
- (f) Storage : Minimum 2.8 TB All flash

(2) **Hyperconverge Server.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server

RESTRICTED

- (d) Computing : Minimum 128 Physical Cores
- (e) RAM Pool : 2 TB
- (f) Storage : Minimum 243 TB All flash

b. **Routers.**

(1) **Core Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 90 Gbps (SD-WAN mode)
- (d) Port : 12 x 1/10 GE, 2 x 40 GE & 2 x 40/100 GE

(2) **Internet/DMZ Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 19 Gbps (SD-WAN mode)
- (d) Port : 4 x 1/10 GE and 8 x 1 GE

(3) **WAN Router.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 19 Gbps (SD-WAN mode)
- (d) Port : 4 x 1/10 GE and 8 x 1 GE

c. **Switch.**

(1) **WAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(2) **Distibution Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(3) **FC/SAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 1 Tbps
- (d) Port : 32 x 32 Gb SW SFP Ports

(4) **Spine Switch.**

RESTRICTED

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 11.5 Tbps
- (c) Port : 28 x 100/40 Gbps, 8 x 400/100 Gbps

(5) **Border Leaf Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.25 Tbps
- (d) Port : 48 x 1/10/25 Gbps

(6) **Leaf Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.25 Tbps
- (d) Port : 48 x 1/10/25 Gbps

(7) **SDN Controller.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.

(8) **DC-DR Replicator Switch (IPN).**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 3.5 Tbps
- (d) Port : 24 x 1/10/25 Gbps

(9) **Out of Band Management Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 170 Gbps
- (d) Port : 48 x 10/100/1000 Base T

d. **Firewall.**

(1) **Core Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(2) **WAN Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 20 Gbps
- (d) Port : 8 x 10 G and 8 x 1/10G SFP+

(3) **DMZ Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(4) **Core Firewall 2.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps
- (d) Port : 8 x 10 G SFP+ and 8 x 1/10/25 G SFP+

(5) **WAN Firewall 2.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 25 Gbps
- (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(6) **DMZ firewall 2.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 25 Gbps
- (d) Port : 4x1G, 8x 1/10 G SFP+ & 4 x 10/25G SFP+

(7) **Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 95 Gbps
- (d) Port : 8x10/25G SFP+ & 2 x 40/100 G

(8) **Application Delivery Controller (ADC), Web Application Firewall & API Security.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 60 Gbps in L7
- (d) Port : 8x10/25G, 2x 40/100 G SFP+ +

e. **Storage Solution.**

(1) **Storage.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Architecture : 02(two) controller update upto 04 controller
- (d) Capacity : 200TB Usable with NVMe hard disk
- (e) Deployment : DC-NDC-DR, sync-sync-async

37. **Active Hardware for UDC (Command HQ & Base).**a. **Server.**(1) **Rack Server Type-2.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Form Factor : 2U Rack Mountable Server
- (d) Computing : Minimum 40 Physical Cores
- (e) RAM Pool : 128 GB
- (f) Storage : Minimum 4.8 TB All flash

(2) **Branch Router Type 1**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 19 Gbps
- (d) Port : 4 x 1 GE WAN and 8 x 1 GE L2

b. **Firewall.**(1) **Branch Firewall Type-1.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 2 Gbps
- (d) Port : 4x1G, 2x 1/10 G
- (e) Users : 200+

(2) **Branch Firewall Type-2.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 2 Gbps
- (d) Port : 4x1G, 2x 1/10 G
- (e) Users : 50-199

(3) **Branch Firewall Type-3.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Throughput : 2 Gbps
- (d) Port : 4x1G, 2x 1/10 G
- (e) Users : 1-49

c. **Switch.**(1) **Distribution Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.

RESTRICTED

- (c) Switching Capacity : 2 Tbps
- (d) Port : 24 x 1/10/25G Ethernet

(2) **POE LAN Switch.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 125 Gbps
- (d) Port : 24 x 10/100/1000 Base T POE+

(3) **Industrial Grade Ethernet Switch (Jetty).**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 125 Gbps
- (d) Port : 8 x 10/100/1000 Base T POE+

38. **Active Hardware for UDC (Ship).**

a. **Router.**

(1) **Branch Router Type 2**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Forwarding Rate : 1 Gbps
- (d) Port : 4 x 1 GE WAN

b. **Firewall.**

(1) **Industrial Grade Firewall.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Firewall Throughput : 790 Mbps
- (d) Port : 4 x 1 GE WAN and 2 x 1 GE SFP

c. **Switch.**

(1) **POE LAN Switch**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Switching Capacity : 125 Gbps
- (d) Port : 24 x 10/100/1000 Base T POE+

Note: The above type and distribution is for preliminary/high level design and cost estimation. However, type of equipment and quantity may change in various data centers based on final approved design by the purchaser. The total quantity as per BOQ shall remain same.

The details technical specification of above mentioned (Article 33-38) active hardware are given in Annex A “Active Hardware CDC DRDC, NHQ DC & Network Room”. Bidder is to comply each parameters mentioned in the Annex A.

Technical Specification of Workstation

39. **Workstation PC**

a. **All in One PC.**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: All-in-one desktop PC
- (4) Country of Origin: As per Article 20
- (5) Country of Manufacture: To be mentioned
- (6) Processor: Intel 12 Gen, Core-i5
- (7) RAM: 16 GB
- (8) SSD: 512 GB
- (9) Screen Size: 24 inch or higher
- (10) OS: Windows 11 Enterprise edition
- (11) Keyboard, mouse and other accessories to be included

b. **NOC & SOC PC**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: Business desktop PC
- (4) Country of Origin: As per article 20
- (5) Country of Manufacture: To be mentioned
- (6) Processor: Intel 12 Gen, Core-i7
- (7) RAM: 32 GB
- (8) SSD: 1TB
- (9) HDD: 4TB
- (10) Monitor Size: 24 inch or higher
- (11) Monitor Qty: 3 per PC with necessary monitor arm
- (12) OS: Windows 11 Enterprise edition
- (13) Keyboard, mouse and other accessories to be included

40. **Printer & Scanner.**

a. **Laser Printer (Colour- A4 , All in one).**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: Print, Scan & Copy
- (4) Country of Origin: As per article 20
- (5) Country of Manufacture: To be mentioned
- (6) Page Per Minute Colour: At Least 21
- (7) Page Per Minute black & white: At Least 21
- (8) Paper Size: Legal & A4
- (9) Duplex: From Day 1
- (10) Automatic Sheet Feeder: From day 1

b. **Laser Printer (Colour- A3).**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: Print: A3 flat bed
- (4) Country of Origin: As per article 20
- (5) Country of Manufacture: To be mentioned
- (6) Page Per Minute Colour: At Least 20
- (7) Page Per Minute black & white: At Least 20
- (8) Paper Size: A3

c. **Laser Printer (Black and White).**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: Print, Scan & Copy
- (4) Country of Origin: As per article 20
- (5) Country of Manufacture: To be mentioned
- (6) Page Per Minute black & white: At Least 21
- (7) Paper Size: Legal & A4
- (10) Duplex: From Day 1
- (11) Automatic Sheet Feeder: From day 1

d. **Scanner.**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Type: Flat bed and Automatic Sheet Feeder
- (4) Country of Origin: As per article 20
- (5) Country of Manufacture: To be mentioned
- (6) Paper Size: Legal & A4

Technical Specification of Software for CDC, DRDC, NHQ DC, UDCs, NOC, SOC, Management and End User PC)

41. **Software.** The data centers and network room shall use various types of software for data processing, data flow and cyber security. The software shall be used in the network are summarized below along with short specification:

a. **OS Software.**

(1) **Server OS License.**

- (a) Brand : Windows
- (b) Manufacturer: Microsoft
- (c) Version : 2025 Standard Edition
- (d) License : Perpetual License

(2) **Server OS License.**

- (a) Brand : Windows
- (b) Manufacturer: Microsoft
- (c) Version : 2025 Enterprise Edition

(d) License : Perpetual License

(3) **Server Client Access License (CAL).**

- (a) Brand : Windows
- (b) Manufacturer: Microsoft
- (c) Version : 2025
- (d) Subscription based for 1 year

(4) **Server OS License.**

- (a) Brand : Linux
- (b) Distribution : RED HAT
- (c) Subscription based for 1 year

b. **Security Related Software.**

(2) **Multi Factor Authentication.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years'
- (d) Function : To enroll multiple devices for authentication.

(3) **Email Security Gateway.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : To support a comprehensive email security solution that integrates inbound and outbound defenses against latest email threats.

(4) **Extended Detection and Response (XDR).**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : Provides integrated threat detection, investigation, and automated response across multiple security layers (endpoints, networks, and servers) to enhance overall cybersecurity defense.

(5) **SIEM & SOAR.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : SIEM tools detect and alert on potential threats, while SOAR platforms help automate the response to those threats.

c. **Access Control Software for Servers.**

(1) **Privileged Access Management (PAM).**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : Enforce end-to-end accountability effectively with every privileged user is accountable to his/her activity on the system

(2) **Active Directory Controller Software.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.

d. **Software for NOC**

(1) **Monitoring Software.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : Plays a crucial role in ensuring the health, performance and security of servers.

e. **Software for SOC**

(1) **Vulnerability Management Software.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : Vulnerability Management Software helps organizations proactively manage the risks associated with vulnerabilities in their systems and networks, reducing the likelihood of successful cyberattacks.

(2) **Active Directory (AD) Security.**

- (a) Brand : To be mentioned.
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : Plays a crucial role in managing and securing network resources, ensuring that only authorized users and devices can access certain data or services.

(3) **Penetration Testing Solution.**

- (a) Brand : To be mentioned
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.

RESTRICTED

(d) Function : a critical component of proactive cybersecurity, providing organizations with the tools and insights they need to defend against increasingly sophisticated cyber threats.

(4) **Server Security Solution.**

- (a) Brand : To be mentioned (Preferably Trend Micro).
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.
- (d) Function : A Server Security Solution integrates various protective measures that ensure servers remain secure from internal and external threats.

(5) **DNS Firewall with DHCP and IPAM.**

- (a) Brand : To be mentioned (Preferably Trend Micro).
- (b) Model : To be mentioned.
- (c) Subscription : 3 Years.

g. **Software for End User PC**

- (1) Windows OS for End User PC (To be included with PC).
- (2) Linux OS for NOC and SOC PC.
- (3) End User - End Point Protection (Antivirus and Anti Malware).

h. **LB/WAF/DDos Management Software.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Subscription : 3 Years.

j. **Backup Software.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Subscription : 3 Years.

Note: Necessary backup software shall be supplied in portable media/CD/DVD along with configutaion file, installation instruction and license key (if needed).

The summary of Software to be supplied along with quantity and distribution are as follows:

Software	CDC	DRDC	NHQ DC	UDC (Comd HQ & Base)	UDC (ship)
OS Software	TBI	TBI	TBI	-	-
Security Related Software	TBI	TBI	TBI	TBI	TBI
Access Control Software for Servers	TBI	TBI	TBI	-	-

RESTRICTED

Software for Data Centre Infrastructure Management	TBI	TBI	-	-	-
Monitoring Software	TBI	TBI	-	-	-
Vulnerability Management Software (SOC)	TBI	-	-	-	-
Active Directory (AD) Security (SOC)	TBI	-	-	-	-
Penetration Testing Solution (SOC)	TBI	-	-	-	-
Server Security Solution	TBI	TBI	TBI	TBI	TBI
Software for Data Center User PC (Qty:04)	TBI	TBI	TBI	-	-
** To be Installed - TBI					

Note: The above distribution may vary based on the actual requirement.

The details technical specification of above mentioned (Article 41) software are given in Annex B "Software-CDC DRDC & PC". Bidder is to comply each parameters mentioned in the Annex B.

TECHNICAL SPECIFICATION OF PASSIVE HARDWARE

Passive Hardware for CDC

42. The CDC shall have various types of passive hardware to support the data centers and network connectivity for uninterrupted operation. The passive hardware shall be used in CDC are summarized below along with short specification:

43. **Rack for Active Devices.**

a. **Server Rack with KVM.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm
- (6) Port : 16

b. **Rack without KVM.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm

c. **Hot-aisle Containment System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature : A common ducting system should be used.

44. **Power Arrangement.**

a. **Automatic Voltage Regulator.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 800 KVA.

b. **Backup Online UPS Stand Alone.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: 250KVA/KW.
- (4) Backup : 30 Minutes

c. **Modular Online UPS .**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: 200KVA/KW with 250KVA Chasis .
- (4) Backup : 30 Minutes

d. **Online UPS Stand Alone.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: 40 KVA/KW.
- (4) Backup : 30 Minutes

e. **Isolation Transformer.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 250KVA.

f. **Floor Mounted Power Distribution System- with Auto transfer Switch for Server room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 200A

g. **Floor Mounted Power Distribution System with Auto Transfer Switch for MMR-01&02.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 100A.

h. **IT Power Distribution Module 3 x 1 Pole 3 Wire 32A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 32A.

j. **IT Power Distribution Module 3 Pole 5 Wire 32A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 32A.

k. **IT Power Distribution Module 3 Pole 5 Wire 63A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 63A.

l. **Rack Automatic Transfer Switch for Single Corded Equipment.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: At least 6 kW or higher.

m. **Transient Voltage Surge Suppression (TVSS).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: Microprocessor-based controller.

n. **Signal Reference Grid System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature : Separate SRGs for server room, power room, MMR.

p. **Data Center Earthing & Bonding System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature : The ground resistance has to be below 1 ohm.

q. **Data Center Infrastructure Monitoring Software (DCIM) with Energy & Environment Monitoring System with BMS.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) No of device license required: At-least 1500 node license.

r. **Controlled Electric Lighting System (Electric lighting & Emergency Lighting).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

s. **Electrical Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Requirement: As per Tier-3 Load flow.

t. **Power Cabling and Other Related Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Requirement: All connection of UPS, AVR, RACK and other electric items (approx. 36 Nos. Rack) inside the data center through IT Power Distribution Modules.

u. **Power Cable Ladder.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Cable ladder size: width 12".
- (4) Height : Approx. 2"/Customized.

v. **Electrical Switch Sockets.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge.

45. **Air Conditioning System.** The chiller and precision air conditioning unit is capable of running separately to fulfill load cooling of server room. As a whole both system will work at N+N configuration of Tier-3 certification.

a. **Precision Air Conditioner (PAC) DX for Server Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 104 kW .

b. **Precision Air Conditioner (PAC) DX for MMR & Power Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 14.8 kW.

c. **Chiller.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: Minimum 260 KW by 2 Unit (N+N) .

d. **Chilled Water (CW) Air Handling Unit for Server Room.**

- (1) Brand : To be mentioned .
- (2) Model : To be mentioned.
- (3) Total Cooling capacity: Minimum 110.2 kW.

e. **Chilled Water (CW) Air Handling Unit for MMR & Power Room**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Cooling capacity: Minimum 16 kW.

f. **Comfort Cooling (VRF for SOC, NOC, Stagging room & Office area with Corridore).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

46. **Fire Fighting System.** Fire Fighting System shall includes the followings:

a. **Very Early Smoke Detection Aspirating (VESDA) System.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: The proposed solution should be for approx 6,000 sqft. Floor space.

b. **Automated Fire Suppression System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) GAS agent: NOVEC-1230.
- (4) Refill: The system should be easily refillable.

c. **Fire Hydrant System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Floor area to be covered as per drawings.

d. **Portable Fire Extinguisher ABC Dry Power.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

e. **Portable Fire Extinguisher CO₂.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

47. **Access Control System.**

a. **Access Control System with Visitor Management System.**

- (1) Brand : To be mentioned.

RESTRICTED

- (2) Model : To be mentioned.
- (3) Requirement: Combination of IRIS (1unit), RFID & Biometric (30 unit) including 31 unit Exit Reader.

b. **Baggage Scanner.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

c. **Turnstile Gate with RFID Access Control Module.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Housing dimension: 1400*270*1000mm,
- (4) Flap arm length: 275mm
- (5) Max arm width: 900mm.

d. **Walk Through Gate.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Detection Zone: 33.

48. **CCTV System.**

a. **Camera.**

- (1) 5 MP Bullet IP Camera
- (2) 5 MP PTZ IP Camera
- (3) 5 MP Dom IP Camera

b. **Network Video Recorder (NVR).** Server based NVR system.

c. **LED TV.** Size: 65 inch.

49. **Other System/ Equipment.**

a. **Raised Floor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor Area: Approx. 6,000sft.

b. **Floor Insulation.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor area : Approx. 6,000sft.

c. **Dry Wall & Paint Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total area: Bidder will proposed as per drawing & requirement.

- d. **Water Leak Detection System (WDS).**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Area to be covered: Bidder will propose as per design & requirement.
- e. **Lightning Protection System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- f. **Rodent System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- g. **NOC with Gallery Type Seating Arrangement.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Gallery: 2 steps
 - (4) Total user: 8
 - (5) Screen Size: 20 ft x 10 ft
- h. **SOC with Seating Arrangement.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Row : 02
 - (4) Total user: 6
 - (5) Screen Size: 14 ft x 10 ft
- j. **Fork-Lift for Equipment Movement.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Load Capacity: 450 kg
 - (4) Lifting Capacity : 7 ft
 - (5) Horizontal Arm extension: Minimum 100mm
- k. **PA System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- l. **Wireless Powered Desktop Laminated Label Printer.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Tape Size: 36 mm
- m. **Dual Sided Card Printer with Ribbons & Cards.**
- (1) Brand : To be mentioned.

- (2) Model : To be mentioned.
- (3) Print Speed: 450 cph

n. **Fire Rated Door for Data Center.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Fire Rating: for 120 Minutes, Conforms to IS3614

50. **Data Center Tier-3 Certification Services.**

- a. Design validation: Tier-3 from Uptime Institute/epi
- b. Data Center Certification: Tier-3 from Uptime Institute/epi

51. **Gensets & Substation.**

a. **Express Line Feeder with RMU & HT Metering Panel.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) For 2X800KVA substation the express line feeder from nearby RMU.

b. **11KV Isolator with Vacuum Contactor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Rated Current: 630 Amps.

c. **HT Automatic Voltage Regulator (AVR) with Bypass Arrangement.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Rated Current: 630 Amps.

d. **11 KV H.T. SWITCHGEAR (VCB).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Rated Current: 630 Amps.

e. **Cast Resin Dry Type Transformer.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Features: 800kVA

f. **Phase Correction Device (PCD).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 1600 A

g. **LT Switchgear.**

- (1) Brand : To be mentioned .

RESTRICTED

- (2) Model : To be mentioned.
- (3) Capacity: 1600 A, ACB with Bus bar Coupler & 2 x MDB-1250A, ACB

h. **480 KVAR Automatic PFI Plant.**

- (1) Brand : To be mentioned (Preferably Schneider Electric, France).
- (2) Model : To be mentioned.
- (3) Capacity: 480 KVAR, 415V, 50 HZ, three phase

j. **Lightning Arresteor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

k. **ATS Panel, 1250A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity:1250A

l. **Bus Bar Trunking System (BBT).**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.

m. **Cables and Connectivity.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Features : Maximum voltage drop shall be less than 2.5%.

n. **Earthing for Substation & Generator.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Features : less than 1 ohm

p. **Fire Fighting System For Sub Station.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

q. **Fire Fighting System For Generator Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

r. **Power System Monitoring-SCADA System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Features : SCADA monitoring system will be established in power distribution network.

- s. **Infrastructure Development Work for Substation and Generator Room.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- t. **Lightning Protection System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- u. **Miscellaneous.** If anything required.
- v. **Generator.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 350 KVA.
- w. **Daytime for Fuel of Generator.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 500L.
- x. **Auto Fuel Refil System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- y. **Underground Fuel Reservoir Tank.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 10,000L.

52. **Ancillary Equipment.** Ancillary equipment to be provided as necessary where Brand, Model and specification are to be mentioned separately.

Passive Hardware for DRDC

53. The DRDC shall have various types of passive hardware to support the data centers and network connectivity for uninterrupted operation. The passive hardware shall be used in the DRDC are summarized below along with short specification:

54. **Rack for Active Devices.**

a. **Server Rack with KVM.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm

(6) KVM Port: 16

b. **Rack without KVM.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm

c. **Hot-aisle Containment System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature : A common ducting system should be used.

55. **Power Arrangement.**

a. **Automatic Voltage Regulator.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 500 KVA.

b. **Modular Online UPS.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: 150KVA/KW with 250KVA Chasis.
- (4) Backup : 30 Minutes

c. **Isolation Transformer.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 200KVA

d. **Floor Mounted Power Distribution System- with Auto transfer Switch for Server Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 100A

e. **Floor Mounted Power Distribution System with Auto Transfer Switch for MMR-01&02.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 50A.

f. **IT Power Distribution Module 3 x 1 Pole 3 Wire 32A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

- (3) Line Current: 32A.
- g. **IT Power Distribution Module 3 Pole 5 Wire 32A.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Line Current: 32A.
- h. **IT Power Distribution Module 3 Pole 5 Wire 63A.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Line Current: 63A.
- j. **Rack Automatic Transfer Switch for Single Corded Equipment.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Capacity: At least 6 kW or higher.
- k. **Transient Voltage Surge Suppression (TVSS).**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Feature: Microprocessor-based controller.
- l. **Signal Reference Grid System.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Feature : Separate SRGs for server room, power room, MMR.
- m. **Data Center Earthing & Bonding system.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Feature : The ground resistance has to be below 1 ohm.
- n. **Data Center Infrastructure Monitoring Software (DCIM) with Energy & Environment Monitoring System with BMS.**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) No of device license required: At-least 1000 node license.
- p. **Controlled Electric Lighting System (Electric lighting & Emergency Lighting).**
- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
- q. **Electrical Works.**
- (1) Brand : To be mentioned.

RESTRICTED

- (2) Model : To be mentioned.
- (3) Requirement: As per Tier-3 Load flow.

r. **Power Cabling and Other Related Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Requirement: All connection of UPS, AVR, RACK and other electric items (approx. 25 Nos. Rack) inside the data center through IT Power Distribution Modules.

s. **Power Cable Ladder.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Cable ladder size: width 12".
- (4) Height : Approx. 2"/Customized.

t. **Electrical Switch Sockets.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge.

56. **Air Conditioning System.** The chiller and precision air conditioning unit is capable of running separately to fulfill load cooling of server room. As a whole both system will work at N+N configuration of Tier-3 std.

a. **Precision Air Conditioner (PAC) DX for Server Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 60 kW .

b. **Precision Air Conditioner (PAC) DX for MMR & Power Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 14.8 kW.

c. **Chiller.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: Minimum 130 KW by 2 Unit (N+N) .

d. **Chilled Water (CW) Air Handling Unit for Server Room.**

- (1) Brand : To be mentioned .
- (2) Model : To be mentioned.

- (3) Total Cooling capacity: Minimum 60 kW.

57. **Fire Fighting System.** Fire Fighting System shall includes the followings:

a. **Very Early Smoke Detection Aspirating (VESDA) System.**

- (1) Brand : To be mentioned
(2) Model : To be mentioned.
(3) Capacity: The proposed solution should be for approx 4000 sqft. Floor space.

b. **Automated Fire Suppression System for DRDC Server, MMR Battery & Power Room.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) GAS agent: NOVEC-1230.
(4) Refill: The system should be easily refillable.

c. **Portable Fire Extinguisher ABC Dry Power.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.

d. **Portable Fire Extinguisher CO₂.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.

58. **Access Control System.**

a. **Access Control System with Visitor Management System.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Requirement: Combination of IRIS (1unit), RFID & Biometric (14 unit) including 15 unit Exit Reader.

b. **Turnstile Gate with RFID Access Control Module.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Housing dimension: 1400*270*1000mm,
(4) Flap arm length: 275mm
(5) Max arm width: 900mm.

c. **Walk Through Gate.**

- (1) Brand : To be mentioned.
(2) Model : To be mentioned.
(3) Detection Zone: 33.

59. **CCTV System.**

a. **Camera.**

- (1) 5 MP Bullet IP Camera
- (2) 5 MP PTZ IP Camera
- (3) 5 MP Dom IP Camera

b. **Network Video Recorder (NVR).** Server based NVR system.

c. **LED TV.** Size: 65 inch.

60. **Others System/ Equipment.**

a. **Raised Floor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor Area: Approx. 4000sft.

b. **Data Center Floor Insulation.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor area : Approx. 4000sft.

c. **Dry Wall & Paint Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total area: Bidder will proposed as per drawing & requirement.

d. **Water Leak Detection System (WDS).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Area to be covered: Bidder will propose as per design & requirement.

e. **Lightning Protection System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

f. **Rodent System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

g. **NOC with Gallery Type Seating Arrangement.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Gallery: 2 steps
- (4) Total user: 8

(5) Screen Size: 20 ft x 10 ft

h. **Fork-Lift for Equipment Movement.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Load Capacity: 450 kg
- (4) Lifting Capacity : 7 ft
- (5) Horizontal Arm extension: Minimum 100mm

j. **PA System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

k. **Wireless Powered Desktop Laminated Label Printer.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Tape Size: 36 mm

l. **Dual Sided Card Printer with Ribbons & Cards.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Print Speed: 450 cph

m. **Fire Rated Door for Data Center.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Fire Rating: for 120 minute

61. **Gensets & Substation.**

a. **Express Line Feeder with RMU & HT Metering Panel.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) For 1x 500KVA substation the express line feeder from nearby RMU.

b. **11KV Isolator with Vacuum Contactor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Rated Current: 630 Amps.

c. **HT Automatic Voltage Regulator (AVR) with Bypass Arrangement.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Rated Current: 630 Amps.

- d. **11 KV H.T. Switchgear (VCB).**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Rated Current: 630 Amps.
- e. **Cast Resin Dry Type Transformer.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Features: 500kVA
- f. **Phase Correction Device (PCD).**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 800 A
- g. **LT Switchgear.**
- (1) Brand : To be mentioned .
 - (2) Model : To be mentioned.
 - (3) Capacity: 800 A ACB with Bus bar Coupler & 2 x MDB-500A, MCCB
- h. **300 KVAR Automatic PFI Plant.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 300 KVAR, 415V, 50 HZ, three phase
- j. **Lightning Arresteor.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- k. **Automatic Transfer Switch.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: 500A
- l. **Cables and Connectivity.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Features : Maximum voltage drop shall be less than 2.5%.
- m. **Earthing & Bonding.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Features : less than 1 ohm
- n. **Fire Fighting System For Sub Station.**
- (1) Brand : To be mentioned.

(2) Model : To be mentioned.

p. **Fire Fighting System For Generator Room.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

q. **Power System Monitoring-SCADA System.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

(3) Features : SCADA monitoring system will be established in power distribution network.

r. **Infrastructure Development Work for Substation and Generator.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

s. **Lightning Protection System.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

t. **Miscellaneous.** If anything required.

u. **Generator.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

(3) Capacity: 250 KVA.

v. **Day Tank for Fuel of Generator.**

(1) Brand : To be mentioned.

(2) Model : To be mentioned.

(3) Capacity: 500L.

62. **Ancillary Equipment.** Ancillary equipment to be provided as necessary where Brand, Model and specification are to be mentioned separately.

Passive Hardware for NHQ DC

63. The NHQ-DC shall have various types of passive hardware to support the data centers and network connectivity for uninterrupted operation. The passive hardware shall be used in the NHQ-DC are summarized below along with short specification:

64. **Rack for Active Devices.**

a. **Server Rack with KVM.**

(1) Brand : To be mentioned

(2) Model : To be mentioned.

- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm
- (6) KVM Port: 16

b. **Rack without KVM.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm

65. **Power Arrangement.**

a. **Automatic Voltage Regulator.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 300 KVA.

b. **Modular Online UPS.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: 100KVA/KW with 250KVA Chasis.
- (4) Backup : 30 Minutes

c. **Floor Mounted Power Distribution System- with Auto transfer Switch for Server Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 100A

d. **IT Power Distribution Module 3 x 1 Pole 3 Wire 32A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 32A.

e. **IT Power Distribution Module 3 Pole 5 Wire 32A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 32A.

f. **IT Power Distribution Module 3 Pole 5 Wire 63A.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Line Current: 63A.

- g. **Rack Automatic Transfer Switch for Single Corded Equipment.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Capacity: At least 6 kW or higher.
- h. **Transient Voltage Surge Suppression (TVSS).**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Feature: Microprocessor-based controller.
- j. **Signal Reference Grid System.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Feature : Separate SRGs for server room, power room, MMR.
- k. **Data Center Earthing & Bonding system.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Feature : The ground resistance has to be below 1 ohm.
- l. **Data Center Infrastructure Monitoring Software (DCIM) with Energy & Environment Monitoring System with BMS.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) No of device license required: At-least 100 node license.
- m. **Controlled Electric Lighting System (Electric lighting & Emergency Lighting).**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
- n. **Electrical Works.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Requirement: As per Tier-3 Load flow.
- p. **Power Cabling and Other Related Works.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.
 - (3) Requirement: All connection of UPS, AVR, RACK and other electric items (approx. 10 Nos. Rack) inside the data center through IT Power Distribution Modules.
- q. **Power Cable Ladder.**
- (1) Brand : To be mentioned.
 - (2) Model : To be mentioned.

- (3) Cable ladder size: width 12".
- (4) Height : Approx. 2"/Customized.

r. **Electrical Switch Sockets.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge.

66. **Air Conditioning System.** The precision air conditioning unit is capable of running separately to fulfill load cooling of server room. As a whole both system will work at N+1 configuration of Tier-2 std.

a. **Precision Air Conditioner (PAC) DX for Server Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 40 kW .

b. **Precision Air Conditioner (PAC) DX for Power Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Capacity: Minimum 14.8 kW.

67. **Fire Fighting System.** Fire Fighting System shall includes the followings:

a. **Very Early Smoke Detection Aspirating (VESDA) System.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Capacity: The proposed solution should be for approx 750 sqft. Floor space.

b. **Automated Fire Suppression System for NHQ DC Server & Power Room.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) GAS agent: NOVEC-1230.
- (4) Refill: The system should be easily refillable.

68. **Access Control System.**

a. **Access Control System with Visitor Management System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Requirement: Combination of IRIS (01unit), RFID & Biometric (01 unit) including 02 unit Exit Reader.

69. **CCTV System.**

a. **Camera.**

- (1) 5 MP Bullet IP Camera
- (2) 5 MP PTZ IP Camera
- (3) 5 MP Dom IP Camera

b. **Network Video Recorder (NVR).** 32 Channel 4 Bay NVR.

c. **LED TV.** Size: 65 inch.

70. **Others System/ Equipment.**

a. **Raised Floor.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor Area: Approx. 800sft.

b. **Data Center Floor Insulation.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total Floor area : Approx. 800sft.

c. **Dry Wall & Paint Works.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Total area: Bidder will proposed as per drawing & requirement.

d. **Water Leak Detection System (WDS).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Area to be covered: Bidder will propose as per design & requirement.

e. **Lightning Protection System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

f. **Rodent System.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.

g. **Fire Rated Door for Data Center.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Fire Rating: for 120 minute

Passive Hardware for UDC-Command HQ & UDC-BASE and Network

71. The UDC-COMDHQ & UDC-BASE shall have various types of passive hardware to support the Network and network connectivity for uninterrupted operation. The passive hardware shall be used in the UDC-COMHQ & UDC-BASE and associated Network are summarized below along with short specification:

72. **Rack for Active Devices.**a. **Server Rack with KVM.**

- (1) Brand : To be mentioned
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm
- (6) KVM Port: 16

b. **Rack without KVM.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Height: 42U EIA-310-D compliant Closed Rack.
- (4) Width : 750mm to 800mm.
- (5) Depth : 1200mm

c. **Rack for Building (Access Switch).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: 9U.

d. **Rack for Floor (Access Switch).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: 9U.

73. **Power Arrangement.**a. **Stand Alone Online UPS.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity: 6KVA.
- (4) Backup Time: 15 minutes.

74. **Air Conditioning System.** The air conditioning unit consists of:a. **AC Controller.**

- (1) Brand : To be mentioned.

RESTRICTED

- (2) Model : To be mentioned.
- (3) Function : Timer based controller for controlling two split AC.

b. **Split AC (min 2.0 ton) for Room Size 200 SFT.**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity : 2.0 ton.

c. **Split AC (1.5 ton).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Capacity : 1.5 ton.
- (4) Room Size : 140 SFT or below.

75. **Access Control Reader (Stand Alone).** 01 x Stand Alone Reader and 01 x Exit Reader with 05 x Access Card to be provided for each UDC.

76. **CCTV System.**

- a. **For UDC.** 03x 4 MP IP Bullet Camera along with 1 x 8 Channel NVR to be provided in each UDC.
- b. **For 400 Access Switch location.** 02 x 2 MP IP Bullet Camera (for Building and Floor Racks) along with 1 x Server Based NVR software installed in the UDC server room.

77. **Other Item.**

a. **3 KVA Online UPS for Different UDCs Building.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.
- (3) Capacity: 3 KVA.
- (4) Backup Time: 15 minutes

b. **1 KVA Online UPS for Different UDCs Floor. .**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.
- (3) Capacity: 1 KVA.
- (4) Backup Time: 15 minutes

78. **Ancillary Equipment.** Ancillary equipment to be provided as necessary where Brand, Model and specification are to be mentioned separately.

Passive Hardware for UDC-SHIP and Network

79. The UDC-SHIP shall have various types of passive hardware to support the Network and network connectivity for uninterrupted operation. The passive hardware shall be used in the UDC-SHIP and Network are summarized below along with short specification:

80. **Rack for Active Devices.**a. **Rack for UDC-SHIP (Friggatte and Corvette) (For Active Devices).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: 25U .

b. **Rack for UDC-SHIP (LPC and OPV) (For Active Devices).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: 15U .

c. **Rack for Ship's Deck and Section (For Access Switch).**

- (1) Brand : To be mentioned.
- (2) Model : To be mentioned.
- (3) Feature: 6U.

d. **Distribution of Racks for Ship.**

- (1) **Jetty Rack (5 x Location).** BN Flotilla CTG (10 X 6U rack), RRB CTG (8 X 6U rack), BNS TITUMIR (5 X 6U rack), BNS Mongla (10 X 6U rack), NU Pagla (2 X 6U Rack)
- (2) **Frigate (7 X Ship).** 1 X 25U Rack for UDC-Ship, 1 X 6U Rack Deck and 2 X 6U rack for Section.
- (3) **Corvette (5 X Ship).** 1 X 25U Rack for UDC-Ship, 1 X 6U Rack Deck and 2 X 6U rack for Section.
- (4) **LPC (2 X Ship).** 1 X 15U Rack for UDC-Ship, 1 X 6U Rack Deck and 1 X 6U rack for Section.
- (5) **OPV (1 X Ship).** 1 X 15U Rack for UDC-Ship, 1 X 6U Rack Deck.
- (6) **Other Types (Ship).** 1 X 15U Rack for UDC-Ship, 1 X 6U Rack Deck.

81 **Access Control Reader (Stand Alone).** 01 x Stand Alone Reader and 1 x Exit Reader with 05x Access Card to be provided for each UDC-Ship.

82. **Other Equipment.**a. **1 X 1 KVA Online UPS, Rack mountable.**

- (1) Brand: To be mentioned
- (2) Model: To be mentioned
- (3) Features: Rack Mountable in 6U or above rack with 600mm depth for UDC-SHIP
- (4) Backup time: 15 minutes.

83. **Ancillary Equipment.** Ancillary equipment be provided as necessary where Brand and Model are to be mentioned.

The details technical specification of above mentioned (article 42–article 83) Passive Hardware are given in Annex C “Passive Hardware CDC Dhaka”, Annex D “Passive Hardware DRDC CTG, NHQ DC & UDCs ”, Annex E “Gensets & Substations CDC” and Annex F “Gensets and Substations DRDC”. Bidder is to comply each parameters mentioned in the Annex C, Annex D, Annex E, Annex F.

INFRASTRUCTURE DEVELOPMENT WORKS

Works for Data Center

84. The data centers and network room shall be prepared by finishing civil works (bricks, plastering, paint works, interior works, lighting, utility connections, bathroom fittings, furniture supply etc) for the installation of passive and active hardware. The bidder has to conduct the site-survey for ascertain the requirements and shall submit the list of works to be done with offer with price details separately. The infrastructure development along with civil works shall be required for complete network are summarized below along with short specification:

85. **Works for CDC.**

- a. Data Center Infrastructure Work.
- b. Cable Containment& Infrastructure Work.
- c. Raised Floor.
- d. Base Elevation for chiller installation

86. **Works for DRDC.**

- a. Data Center Civil and Infrastructure Work
- b. Cable Containment& Civil Infrastructure
- c. Raised Floor
- d. Pre fabricated building for genset & Substation (2nd storied building, size: 800 sft in each floor)

87. **Works for NHQ-DC.**

- a. Data Center Civil and Infrastructure Work.
- b. Cable Containment& Civil Infrastructure.
- c. Raised Floor.

88. **Works for UDC-COMHQ and UDC-BASE**

- a. Aluminium Glass Partition.
- b. Close the glass windows using PVC Board.
- c. Paint Works
- d. Insulation MAT for Floor
- e. Single bore earthing (< 1 ohms)

89. **Works for UDC(SHIP)**

- a. Aluminium Glass Partition
- b. Welding and Cutting
- c. Insulation MAT for Floor

90. **Furnitures for CDC, DRDC, NHQ DC and UDC (Command HQ, Base and Ship).**

- a. **Interior.** The bidder shall facilitate the datacenter rooms with necessary interior works and lightning equipment.
- b. **Furniture and Ancillary Equipment.** The Bidder shall furnish all the equipment rooms, Power room, NOC (for CDC & DRDC), SOC (for CDC) and administrator room with necessary ancillary equipment (Air condition, Surge protection etc) and office room with appropriate furniture (Brand: HATIL/ AKTER, best quality) as per corporate standard.

The details technical specification of above mentioned (article 84- annex 90) civil works are given in Annex G "Civil Works CDC" and Annex H "Civil Works DRDC". Bidder is to comply each parameters mentioned in the Annex G & Annex H.

CABLING WORKS - FIBER OPTICS AND UTP CABLING

Structure Cabling (Fiber Optics and UTP)

91. **Cabling of CDC, DRDC & NHQ.**

- a. **CAT6A UTP LSZH Cable.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
 - (3) Per Box 305 Meter.
- b. **CAT6A UTP Patch Panel 24 Port Loaded.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
 - (3) Patch Panel: 24 port.
- c. **CAT6A UTP Patch Cord, 10M.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- d. **CAT6A UTP Patch Cord, 12M.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- e. **CAT6A UTP Modular (RJ-45).**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- f. **Work Area Face Plate.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- g. **Modular Fiber Panel, 1U Intelligent Ready.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- h. **Modular Fiber Panel, 4U Intelligent Ready.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- j. **Pre-Terminated MPO Modules.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- k. **2 x 12F MPO Trunk Cable, OM4, 12 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- l. **2 x 12F MPO Trunk Cable, OM4, 15 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- m. **2 x 12F MPO Trunk Cable, OM4, 18 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- n. **2 x 12F MPO Trunk Cable, OM4, 20 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- p. **2 x 12F MPO Trunk Cable, OM4, 22 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- q. **2 x 12F MPO Trunk Cable, OM4, 25 meters.**
 - (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.

- r. **2 x 12F MPO Trunk Cable, OM4, 30 meters.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- s. **LC – LC Multimode Duplex Fiber Patch Cord, 8 Meters.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- t. **LC – LC Multimode Duplex Fiber Patch Cord, 10 Meters.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- u. **Intelligent Upgrade Kit, Copper Panels.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- v. **Intelligent Upgrade Kit, Fiber Panels.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- w. **Intelligent Rack Controller.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- x. **Intelligent System Software, Per Port License.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- y. **Fiber Guide Pathway System.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- z. **Copper Wire Basket Pathway System.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- aa. **Power Cabling.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- ab. **Overhead Hanging Cable Tray for Network Cables.**
- (1) Brand: To be mentioned.
 - (2) Model: To be mentioned.
- ac. **Fiber cable runner.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

ad. **Cable Laying Service.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

ae. **Cabling Accessories.** Standard cabling Accessories (Fiber and UTP). for installation and operation is to be provided as necessary.

92. **Cabling of All UDCs (Command HQ, Base & Ship).**

a. **CAT 6 UTP LSZH Cable.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.
- (3) Per box 305 Meter

b. **CAT6 Patch Panel 24 Port (1U).**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

c. **CAT6 UTP Modular (RJ-45).**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

d. **CAT6 UTP Patch Cord, 1meter.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

e. **CAT6 UTP Patch Cord, 2meter.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

f. **CAT6 UTP Patch Cord, 3meter.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

g. **CAT6 UTP Patch Cord, 10meter.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

h. **CAT6A Modular Faceplate.**

- (1) Brand: To be mentioned.
- (2) Model: To be mentioned.

- j. **CAT6 F/UTP Double Jacketed Outdoor Cable for Ship & Jetty.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- k. **CAT 6 F/UTP Outdoor Patch Cord for Jetty.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- l. **6 CORES – Singlemode Outside Plant Fiber Cable.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- m. **1U Fiber Rackmount Shelf, Sliding.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- n. **Rolo Splice Kit.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- p. **12F LC SM Splice Cassettes.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- q. **6F SM LIU FULLY LOADED, 1U.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- r. **LC – LC Singlemode Duplex Fiber Patch Cord 3 meters.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- s. **Cable Laying Service.**
(1) Brand: To be mentioned.
(2) Model: To be mentioned.
- t. **Cabling Accessories.** Standard cabling Accessories (Fiber and UTP). for installation and operation is to be provided as necessary.

The details technical specification of above mentioned Cable laying service (article 91 - article 92) are given in Annex J “Cabling Fiber and UTP”. Bidder is to comply each parameters mentioned in the Annex J.

DATA LINK SERVICES – NTTN LINKS

93. **Data Link- NTTN.** The bidder is to provided dedicated data link services for connecting remote sites where Purchaser fiber optics link is not aviable. The bidder is to

RESTRICTED

mention the one time installation cost and monthly as well as yearly recurring cost of the dedicated bandwidth. The link should be highly secured considering the military data protection requirement and policy. Sources and desination points must be encrypted with dynamic key or coding. The service shall be provided from NTTN service provider as per the following requirement and Specification:

- a. **CDC to DRDC.**
 - (1) No of path: 2
 - (2) Port Speed: 2 x 10G, 2 x 8G, 2 x 10G, 2 x 1G
 - (3) Data Bandwidth: 1GB, 4GB, 4GB, 100 MB

- b. **CDC to NHQ DC.**
 - (1) No of path: 2
 - (2) Port Speed: 1 x 10G, 1 x 8G, 1 x 10G, 1 x 1G
 - (3) Data Bandwidth: 1GB, 4GB, 4GB, 100 MB

- c. **NHQ DC to DRDC.**
 - (1) No of path: 2
 - (2) Port Speed: 1 x 10G, 1 x 8G, 1 x 10G, 1 x 1G
 - (3) Data Bandwidth: 1GB, 4GB, 4GB, 100 MB

- d. **CDC/NHQDC/DRDC to UDC-COMDHQ.**
 - (1) No of Location: 11
 - (2) No of Path: 02 for each location
 - (3) Port Speed: 1 x 1G
 - (4) Data Bandwidth: 20 MB

- e. **CDC/NHQDC/DRDC to UDC-BASE.**
 - (1) No of Link: 17
 - ((2) No of Path: 02 for each location
 - (3) Port Speed: 1 x 1G
 - (4) Data Bandwidth: 20 MB

- f. **CDC/NHQDC/DRDC to UDC-SHIP.**
 - (1) No of Link: 15
 - (2) No of Path: 02 for each location
 - (3) Port Speed: 1 x 1G
 - (4) Data Bandwidth: 20 MB

The details technical specification of above mentioned (article 93) Data link services are given in Annex K "Data Link NTTN". Bidder is to comply each parameters mentioned in the Annex K.

TOOLS AND TEST EQUIPMENT

94. **Tools and Test Equipment.** The bidder is to offer 02 sets of tools and test equipment for CDC and DRDC which will be used for scheduled and unscheduled maintenance.

Ser	Equipment Name	Qty
1.	SimpliFiber® Pro Optical Power Meter and Fiber Test Kits	02 sets
2.	MultiFiber™ Pro Optical Power Meter and Fiber Test Kits	
3.	OptiFiber® Pro OTDR	
4.	LinkIQ Cable + Network Tester	
5.	Fiber Optic Cleaning Kits	
6.	Visual Fault Locator (VFL)	
7.	NAVITEK NT – NETWORK CABLE TESTER	
8.	Pro'sKit® UTP/STP Cable Stripper	
9.	Network Installation Tool Kit	
10.	Network Repair Tools with tool box	
11.	Hammer, Wrench and Drivers Tools with tool box	

The details technical specification of above mentioned Tools and Test Equipment service are given in Annex L “Tools and Test Equipment”. Bidder is to comply each parameters mentioned in the Annex L.

95. **Spares Parts and Consumables.** The bidder is to offer necessary spares, consumable items for the scheduled and unscheduled maintenance of the BNNET-P1 system.

a. **Spares and Consumables.**

Serial	Description	Quantity	Technical specification
1.	Branch Router Type 1	02 in no	As per technical specification mentioned in the tender document Annex A
2.	Branch Router Type 2	03 in no	
3.	Branch Firewall Type 1	01 in no	
4.	Branch Firewall Type 2	01 in no	
5.	Branch Firewall Type 3	01 in no	
6.	Distribution Switch	02 in no	
7.	Media Converter (10G)	20 Pair	

b. **Spares and Consumables (Optional).**

Serial	Description	Quantity	Technical specification
1.	Branch Router Type 1	02 in no	As per technical specification mentioned in the tender document Technica Annexures
2.	Branch Router Type 2	03 in no	
3.	WAN Firewall	06 in no	
4.	Core Firewall 2	06 in no	
5.	Branch Firewall Type 1	01 in no	
6.	Branch Firewall Type 2	01 in no	
7.	Branch Firewall Type 3	01 in no	
8.	Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security	02 in no	
9.	UDC POE LAN Switch	200 in no	
10.	Distribution Switch	02 in no	
11.	WEB Security Appliance (WSA)	02 in no	
12.	Backup Online UPS Stand Alone-250KVA/KW	02 in no	

RESTRICTED

12.	All in One PC	200 in no	
13.	Media Converter (10G)	20 Pair	
14.	Certified Information Systems Security Professional (CISSP)	Lot	
15.	Certified Information Systems Auditor (CISA)	Lot	

96. **Standard Accessories.** The bidder is to offer necessary standard accessories to install and commissioning the BNNET-P1 system.

INSTALLATION

97. **Site-Preparation and Room Arrangement.** The Bidder shall make necessary arrangement to prepare the Data centers (CDC/DRDC/UDC) for uninterrupted operation of network components. The Bidder will be solely responsible for all the site preparation work such as earthing, laying of underground cables in conduit metal pipes, welding/ cutting etc., for the installation of BNNET-P1 equipment at each Project sites including minor civil, electrical and other works. The requirements related to the site-preparation and room arrangement are as follows:

a. **Drawing and Design.** The bidder shall survey the site and prepare the necessary layout, drawing and design of each type of data center in each location separately. All drawing/ design (including 3D design) is to be vetted by the BN project implementation team along with appointed consultant before implementation. The SUPPLIER will arrange briefing/ presentation in NHQ time to time and before vetting the design and drawings. The approval of designs/ drawings (including 3D design) or observations will be given by NHQ in consultation with the nominated Consultant within two weeks by a 'letter of approval' or by a 'letter of observation'. The observation given by the consultant in any stage of construction work will be addressed by the SUPPLIER without incurring any additional cost to the purchaser.

b. **Power Supply Arrangement.** The Bidder shall arrange the power supply connection from nearest main power distribution box (MDB) to CDC/DRDC/UDC. The purchaser shall facilitate to get the required supply from MDB (400 V AC, 50 Hz, 3 phase/ 220 V, 50 Hz, 1 phase) to CDC/UDC. SUPPLIER shall have to calculate and mentioned the necessary power requirement in the offer. Power arrangement from the designated MDB to CDC/DRDC/UDC shall be the responsibility of Bidder. Necessary generator shed need to be constructed if shed is not available in the CDC/DRDC/UDC site. Power system shall have adequate surge protection devices (SPD) to protect from over-current/ overvoltage. There shall be proper earthing and lightning arrester system for building to protect from thundering.

98. **Installation Material, Fitting, Fixtures and Accessories.** The bidder shall provide all necessary installation material fitting, fixtures and accessories for installation of active hardware, passive hardware and civil works.

99. **Installation.** The Bidder shall employ the expert installation team comprising suitable network experts including power engineer for the assembly and installation of BNNET-P1. BN will not be responsible for the engineering works at assembly sites. BN technicians are to be trained while installing the BNNET-P1.

100. **Employment Responsibility of Installation Engineer by BIDDER.** All costs for installation including food, accommodation and internal transportation of specialist are to be borne by the Bidder. However, on request of Bidder, BN may arrange food and

RESTRICTED

accommodation (subject to availability of such facilities). In that case Bidder is to pay the necessary bills to BN as per BN Mess regulations.

101. **Provision for Future Integration.** BNNET-P1 shall have provision for the following integration in future:

- a. Integrational Tactical Radio Link (Bijoy-50) (ethernet Port)
- b. Integration with IP PABX (Ethernet Port)
- c. Integration with AFD, Sister Services and BCG (Ethernet Port)

102. **Additional Items/ Accessories (If Any).** If any item(s) is not specified but required for the full range operation of BNNET-P1, then the BIDDER shall have to provide such item.

LAYOUT AND PUBLICATIONS

103. **Layout, Drawing, Manual and Publication.** The Bidder shall provide 04 (Four) sets of layout diagram for each type of datacenter (CDC/DRDC/UDCs) including NOC and SOC. The bidder shall have to provide 04 (four) sets of publications (Operator/user manual, maintenance manuals, Wiring Diagram and parts catalogue) of the hardware and software in 2 set X hard copy and 2 set X soft copy in English for each datacenter under the scope of this tender. Bidder is to submit the list of drawing and layout, manual, publication to be supplied with the offer.

TRAINING PACKAGE- FOREIGN AND LOCAL

104. **Training Package.** Training package shall be arrangement in Bidder premises/ recognized training institution in Bangladesh/abroad and on-site if possible. The complete training schedule along with pre-requisites of trainee (if any) is to be submitted with offer. The bidder shall also submit the content of training to be covered and evaluation method to be followed in the training proposal. The basic level foreign and local training shall be completed before the setting-to-works of active hardware. The summary of training package is to be provided by the bidder are as follows:

a. **Foreign Training Package**

Training Category	Training Module	Category of Personnel	Group	Training Premises & Duration
1. Intermediate IT Training – Project Management	Project Management Professional (PMP)	8 X Officer	Group-1	Malaysia (02 weeks)
2. Intermediate IT Training – Facilities Operation	Certified Data Centre Facilities Operations Specialist (CDFOS)	5 X Officer 5 X Sailor	Group 2 5 x Officer & 5 x Sailor will undergo CDFOS and CDFOM training.	Malaysia/Thailand (05 Days)
	Certified Data Center Facilities Operations	5 X Officer 5 X Sailor		Malaysia/Thailand (05 Days)

RESTRICTED

	Manager (CDFOM)			
3. Advanced IT Training – IT Management	ITIL4 Foundation	6 X Officer	Group 3 (6 x Officer will undergo this training 7 days training package)	Malaysia/Thailand (03 days)
	ITIL 4 Specialist	6 X Officer		Malaysia/Thailand (04 days)
4. Cyber Security Training	Certified Information Systems Security Professional (CISSP) (Optional)	6 X Officer	Group -4 6 x Officer will undergo total 2 weeks training package	Malaysia/ Singapore (10 Days)
	Certified Information Systems Auditor (CISA) (Optional)	6 X Officer		Malaysia/ Singapore (5 days)
	Certified Ethical Hacker (CEH)	6 X Officer		Malaysia (2 weeks)

b. **Local Training Package**

Training Category	Training Module	Category of Personnel	Training Premises & Duration
1. Basic IT Training – Technical Support Specialist	Data Centre Operational Support Training	5 X Officer 15 X Sailor	Bangladesh (05 Days)
	Cisco Certified Network Associate (CCNA)	10 X Officer 10 X Sailor	Bangladesh (4 weeks)
2. Intermediate IT Training – System Administrator	Microsoft Certified-Server Administrator	5 X Officer 5 X Sailor	Bangladesh (2-3 weeks)
	Red Hat Certified-Server Administrator	5 X Officer 5 X Sailor	Bangladesh (2-3 weeks)
	Hyperconverge operational Training	5 X Officer 5 X Sailor	Bangladesh (5 days)
3. Advanced IT Training – Network System Administrator	Cisco Certified Network Professional (CCNP) Data Center	4 X Officer 1 X Sailor	Bangladesh (2 months)
	Cisco Certified Network Professional		Bangladesh (2 months)

RESTRICTED

	(CCNP) Enterprise		
4. Advance IT Training – Network Security Analyst	Cisco Certified Network Professional (CCNP) Security	5 X Officer	Bangladesh (2 months)

The details technical specification of Training services are given in Annex M “Training Package Foreign and Local”. Bidder is to comply each parameters mentioned in the Annex M.

105. **Admin Assistance.** All admin costs (Both way return Air fare, Boarding and Lodging, Local transport) related to training in Bidder designated foreign location shall be borne by the bidder. All training related cost (Books, lab guide, stationary and training aids) shall also be born by the bidder. The bidder is to quote the admin cost separately, specially the per day cost of boarding, lodging and internal transport for each trainee.

106. **Terms and Conditions Related to Training.**

- a. On completion of successful training, each trainee will be given with a completion certificate.
- b. The mode of instruction will be in English/Bengali. All documents will be written in English and training aids and materials shall be provided by the Bidder.
- c. Detail plan and course content will be formulated and forwarded to PURCHASER for approval at least 02 months prior commencement of training.
- d. The bidder will provide necessary training materials to support the training.
- e. For all vendor certified training, the bidder should provide exam voucher at the end of the training for all the participants to be certified by the certification authority.
- f. Necessary training will start after signing the contract.

MAINTENANCE SUPPORT

107. **Maintenance Support During Warranty Period.** The BIDDER shall have to employ a qualified support team at each site namely CDC, DRDC & UDC (Comkhul) at least of 03 people (02 for passive equipment, 1 for active equipment for 24/7) during the warranty period (i.e 12 months after the acceptance). The bidder is to maintain the pool of manpower for employing at each site 24/7. The maintenance support service during the warranty period shall be quoted separately in the financial offer. The responsibilities of the bidder’s maintenance support service and maintenance support personnel are as follows:

- a. Routine maintenance of all equipment.
- b. Diagnosis, troubleshooting and repair of all equipment.
- c. Software troubleshooting and configurations.
- d. Train BN personnel on network operation and maintenance.
- e. To raise the warranty for the unserviceable item and expedite the restoration process.

- f. The Bidder will maintain sufficient backup stock of spare parts and tools locally at sites, for the maintenance of the supplied equipment, during the warranty period.
- g. The Bidder will ensure availability of spare parts and technical assistance for all components for at least 02 (two) years, without major changes, after the completion of final acceptance.
- h. The bidder will give six months advance notice on any discontinued part(s) with a suggestion for appropriate alternatives.

108. **Maintenance Support Service after the Warranty Period.**

- a. **Annual Maintenance Contract (Optional).** The bidder is to offer 05 (five) years annual maintenance contract after the warranty period. The AMC will cover employment of personnel at each site (3) CDC, DRDC, UDC(COMDHQ, Khulna) for troubleshooting, preventive maintenance, disaster recovery and regular maintenance services. The bidder is to quote price of each year separately as optional. The Purchaser shall select the duration of AMC based on the requirement. The purchaser may extend the duration of service or renew the contract each year following the existing service procurement regulation of BN.
- b. **On Call Engineer’s Support from OEM.** This support will be needed for any unscheduled repair/ maintenance of the equipment after the warranty period.

PART-3: GENERAL TERMS AND CONDITIONS

INSPECTION AND ACCEPTANCE

109. **Inspection and Acceptance.** Bidder will submit two copies of Bidder’s test results of the BNNET-P1 equipment and related facilities to the purchaser not less than two weeks prior to the commencement of the acceptance tests.

- a. **FAT / PSI.** The Factory Acceptance Test (FAT) and Pre Shipment Inspection (PSI) shall be carried out in accordance with standard acceptance procedure of PURCHASER. The items for which the FAT/PSI will be required are as follows:

Ser	Item	Remarks
1.	Generator	FAT
2.	UPS (250KVA, 200 KVA, 100KVA)	PSI

Following FAT/PSI criteria to be complied by the bidder to conduct FAT/PSI:

- (1) FAT/PSI shall be carried out by a team of 03 (Three) BN members for duration of 03 (Three) working days in each OEM premises at the purchaser’s expense. Both way air fare, accommodation and food for the FAT/PSI team shall be borne by Purchaser. All types of movement/ transportation (air/sea/road) of the team within the manufacturer’s country, reception and arrangement for entry into the country/ concerned area for the FAT/PSI are to be arranged by the bidder. The bidder should inform the purchaser about the date of FAT/PSI (schedule) and FAT/PSI criteria at least 08 (eight) weeks prior to the date of FAT/PSI. FAT/PSI procedure shall be forwarded to the

RESTRICTED

purchaser 6 (six) weeks prior to the date of commencement of the FAT/PSI to the concerned directorate (DNIT, NHQ) for approval of BN.

(2) On return from the country of manufacturer, the FAT/PSI team will submit the joint FAT/PSI report to concerned Directorate (DNIT, NHQ) at Naval Headquarters.

(3) The FAT/PSI shall be carried out at manufacture's factory premises following approved FAT protocols. In this regard, the FAT protocol is to be approved by Purchaser well in advance.

b. **Testing/ Trial Run.** On completion of the installation of the system, the same is to be given trial run and operation for at least 30 (thirty) days in presence and under direct supervision of Bidder's technical experts at BN site. The installation Engineer should be available at the site during whole period of the working hours and remain stand-by for on-call service after cease hours. The Bidder is to rent sufficient NTTN bandwidth for test and trial run for 30 days at Bidder's cost. If trial run is extended due to Bidder's requirement, extended trial run period will be covered by the Bidder's cost.

c. **Commissioning of the Project.** The BNNET-P1 equipment setup is to be commissioned and handed over to BN in fully operational condition without any observation. If the system is found unsatisfactory, acceptance check will be held up till the equipment/hardware/system is made serviceable by the Bidder.

d. **BNNET-P1 Civil Works Completion Certificate.** The user will provide 'Civil Work Completion Certificate after successful completion of all kind of civil works (site preparation, brick works, insulation, dry wall, door, windows, flooring, furniture, interior work, painting, plumbing, utility connection and any other related infrastructure work required to meet the specified standards and design criteria) of CDC, DRDC, NHQ DC and UDC mentioned in tender specifications.

e. **Certificate of Receiving LOT Passive Item.** The purchaser will issue the Certificate upon submission and inspection by CINS/ ACINS, provided that at least 50% value of the total cost of passive items has been met. All the items will be inspect visually according to the packing list in the presence of supplier, consultant and acceptance committee of BN.

f. **BNNET-P1 Fiber Optics Cable Laying Completion Certificate.** The Fiber Optics Cable Laying Certificate will be issued upon the successful installation, testing, and commissioning of the fiber optic cable in all Data Centers, Bases and Ships mentioned in the tender specification. This includes trenching, duct installation, cable pulling, splicing, boring, termination, and signal testing to confirm full operational readiness and adherence to the project's specifications and quality standards. The bidder is to prepare the final layout after the cable laying works using geo-tagging mapping system and will provide 2 X printed copy and 1 X soft copy to the purchaser.

g. **BNNET-P1 Structure Cabling Completion Certificate.** The Structure Cabling Certificate will be issued upon the successful installation, testing, and commissioning of Cabling from Data Centers to user end and inside Data Center mentioned in the tender specification. The bidder is to prepare the final layout after

the cable laying works using suitable software and will provide 2 X printed copy and 1 X soft copy copy to the purchaser.

h. **CDC and DRDC Power Supply Arrangement Setting-to-Work Completion Certificate.** The Power Supply Arrangement Setting-to-Work Completion Certificate will be provided after the successful installation, testing, and commissioning of the power supply systems for both CDC and DRDC. This includes the setup of substation, generators, AVR, transformers, UPS systems, wiring, earthing, and backup power solutions. All components must be tested for operational integrity, reliability, and compliance with the approved design and safety standards, ensuring full functionality to support uninterrupted power to both facilities. Necessary installation layout and diagram shall be prepared by the bidder and will provide 2 X printed copy and 1 X soft copy copy to the purchaser.

j. **CDC and DRDC Air Conditioning Setting-to-Work Completion Certificate.** The Air Conditioning Setting-to-Work Completion Certificate will be issued upon the successful installation, testing, and commissioning of the air conditioning systems for CDC and DRDC. This includes the setup of chiller installation, PAC installation, VRF system, indoor and outdoor units, ducting, insulation, electrical connections, controls etc as per design and drawing. Necessary installation layout and diagram shall be prepared by the bidder and will provide 2 X printed copy and 1 X soft copy copy to the purchaser.

k. **Certificate of Receiving all Active Hardware Item.** This certificate will be given upon submission and inspection of all active hardware items to CINS/ ACINS office . All the items will be inspected visually according to the packing list in the presence of supplier, consultant, representative of CINS/ACINS and acceptance committee of BN. A joint inspect report is to be prepared and submitted by the bidder.

l. **Certificate of Receiving Workstation PC.** This certification will be given after submission and inspection of all workstation to CINS/ ACINS office. All the workstations will be inspected visually according to the packing list in the presence of supplier, consultant, representative of CINS/ACINS and acceptance committee of BN. A joint inspect report is to be prepared and submitted by the bidder.

m. **Subscription Certificate of BNNET-P1's Software.** This certificate will be provided upon getting the subscription activation notification via Email/ Portal. A joint inspect report is to be prepared and submitted by the bidder.

n. **Setting-to-Work Certificate of BNNET-P1's Software.** This certificate confirms the successful installation, configuration, and initial testing of BNNET-P1 software mentioned in the tender specification. All components have been set up according to specifications, and basic functionality has been verified to ensure that the software is operational and ready for further testing or use. A joint inspect report is to be prepared and submitted by the bidder.

p. **Foreign Training Completion Certificate.** This certificate will be provided after successful completion of each basic, intermediate and advanced foreign training mentioned in tender requirements.

q. **Local Training Completion Certificate.** This certificate will be provided after successful completion of each basic, intermediate and advanced Local training mentioned in tender requirements.

r. **Final Acceptance Certificate.** After successful trial run and certification by Tier-3 authority, final acceptance check shall be carried out by the bidder's and purchaser's team. The bidder shall prepare the complete inventory of the BNNET-P1 including drawing, design and publication before 01 week of final acceptance commencing date. Both team shall jointly complete the inspections with help of consultant and sign the final acceptance certificate for commissioning and handover the BNNET-P1 project.

Shipment and Transportation

110. **Packing.** BNNET-P1 and its equipment should be packed in such a way that those should be transported by air, land and sea (as applicable). The package is to provide BNNET-P1 (and its components) protection from the external mechanical and environmental factors exposure during its transportation and storage. The manufacturer will pack the equipment in accordance with the packaging instruction. In case total or partial preservation is required, the manufacturer will apply temporary anti-corrosive protection (preservation) to the equipment in accordance with the correspondent instructions.

111. **Transportation.** The BNNET-P1 and its associated items are to be delivered to the BN site at Chattogram (in case of shipment by sea):

Consignee: The Commanding Officer, Naval Stores Depot, Chattogram, New Mooring, Chattogram, Bangladesh), and

Or at NSSD, Dhaka (in case of shipment by air):

Consignee: Officer In-charge, Naval Stores Sub Depot Dhaka, Namapara Khilkhet, Dhaka 1229.)

All removable segments must have appropriate safe packaging for transportation. The SUPPLIER is also to bear the expenditure for internal transportation from the port of entry to respective BN sites (CDC/RDC/UDC-SR/UDC-R). All cost related to transportation from sea port/airport/NSD CTG/NSSD Dhaka to designed installation site/user location shall be borne by the bidder.

112. **Security Clearance.** BN will arrange security clearance for the Bidder's specialists to conduct pre-bid and post bid site-survey activities and installation as well as technical support of BNNET-P1 project. The list of the team members along with necessary information is to reach NHQ (Directorate of Naval IT) at least 30 days before the date of arrival of bidder team. The bidder is to submit necessary bio-data in the prescribe form to NHQ (DNIT) for the security clearance of bidder personnel.

113. **Obsolescence.** If any system, equipment etc becomes obsolete or out of production during the installation period, the Bidder is to submit a minimum of 03 (three) alternatives of same/improved version with brochure/Catalogue/Technical data sheet for selection of suitable replacement by the Purchaser without any additional cost.

114. **Delivery.** One complete set of BN Network System along with all Hardware, Software, Software License and Accessories are to be delivered, installed and commissioned within 12 (twelve) months from the date of signing the contract as per scope

RESTRICTED

of supply. **Partial delivery shall be allowed.** The bidder is to submit the calculated timeline considering the delivery period as per the following format:

Serial	Milestone	Required Time	Completion Calender days
	Contract Signing Date	D day	Example: 01 April 2024
1.	Site-survey and submission of Survey report with design, drawing and Installation layout of BNNET-P1.	D+15 Days	Example: 15 April 2024
2.	Submission of Tier-III Certified Design and Layout Approval Certificate for Central Data Center from Uptime USA or Equivalent org		
3.	BNNET-P1 Civil Works Completion		
4.	FAT and PSI schedule		
5.	Receiving LOT Passive Item		
6.	Submission of BNNET-P1 Fiber Optics Cable Laying Completion Report		
7.	Submission of BNNET-P1 Structure Cabling Completion Report		
8.	Submission of CDC and DRDC Power Supply Arrangement Setting-to-Work Completion Report		
9.	Submission of CDC and DRDC Air Condition Setting-to-Work Completion Report		
10.	Receiving all Active Hardware Item		
11.	Receiving Workstation PC		
12.	Receiving of Subscription Certificate of BNNET-P1's Software		
13.	Submission of Setting-to-Work Certificate of BNNET-P1's Software		
14.	Submission of Foreign Training Completion Report		
15.	Submission of Local Training Completion Report		
16.	Submission of Installation, Integration with VSAT link (if installed and run) and Trial-run Report		
17.	Submission of Tier-III Certification from Uptime Institute (USA) for CDC		
18.	Submission of Final Acceptance Report of Spare, Tools and Test Equipment		
19.	Submission of Final Acceptance Certificate of the BNNET-P1		

Warranty and After Sales Services

115. **Warranty.**

a. **Warranty Period.** Warrantry services will be as follows:

(1) **Warranty of BNNET-P1 System.** 12 months from the date of acceptance.

RESTRICTED

(2) **Warranty of the Hardware.** As per the extended (2-3 years) warranty provided by the OEM.

(3) **Warranty of the Software.** As per the extended (3 years) warranty/subscriptions/ License provided by the OEM.

b. **Warranty Services.**

(1) Any unserviceable incident up to 24 (twenty-four) hours will be deemed as normal. But more than 24 hours will be deducted from the warranty period.

(2) Replacement/ Repair of defective equipment or services, if needed during inspection/ warranty period, the SUPPLIER is to provide the same free of cost within 01 (one) months from the date of reporting. Freights and Insurance charges for both the ways and cost for site visit by manufacturer engineer (if needed) are to be borne by the SUPPLIER. Warranty will extend if replacement/repair time limit exceeds 45 days from the date of reporting by the End User (BN).

(3) Warranty of Software/licenses can not be less than 2.5 (three years). Warranty of other items should be minimum 2.5 years

c. **Guaranty for Spare Support.** 10 years of spares support assurance are to be provided by the manufacturer of the BNNET-P1.

d. **Technical Advisory Service.** The technical advisory service through electronic or conventional mail or online servicing (if available) from the factory/ OEM office will be provided by the manufacturer during the warranty period and after warranty period as and when required. The address, email, contact details with procedure will be provided within 02 weeks of signing the contract.

116. **Miscellaneous Terms and Conditions.** The following miscellaneous terms and conditions are to be followed:

a. Supplier will ensure its local presence and maintain technical support team (TST) for maintenance and technical support on 24/7 basis and as and when required by BN during the warranty period.

b. Due to the fault of the SUPPLIER, if any changes/ amendment is required in the contract/ Total Contract Price (TCP) , all such expenses/ charges will be borne by the SUPPLIER.

c. The cost of BNNET-P1 and additional equipment including all charges is to be "Firm and Fixed". No increase of price at any stage after signing the contract will be accepted. If any item other than those already contracted is required during installation of BNNET-P1, those are to be provided by the SUPPLIER within the contracted price.

Payment Terms

117. **Performance Guarantee (PG)/Pay Order.** The BIDDER shall furnish a Performance Guarantee (PG) with validity from the date of expiry of the delivery schedule (as per DGDP format in local currency) in the shape of Bank Guarantee (applicable only for the Industries/ Factory/ Organization under Armed Forces and Government) and in the shape of Pay Order (other Industries/ Factory/ Organization etc) as security. The PG is of (Amount is to be as per existing DGDP rules) on the Total Contract Price (TCP) in favour of The Senior Finance Controller (Navy), Sailors Colony, Lalasarai, Mirpur-14, Dhaka-1206 as security

RESTRICTED

money through any scheduled bank located in Bangladesh. In all the cases, PG should be submitted before signing the contract. The **PG shall be released by the SFC(Navy) on receipt of Final Acceptance Certificate from DGDP**. If the contractual obligation warrants the extension of validity of PG, the BIDDER shall remain liable to do so at his own cost.

118. **Terms of Payment.** Total 100% payment amounting Taka (To be mentioned during contract sign) shall be made in local currency by PURCHASER against bills/documents submitted by the SUPPLIER/ BIDDER through DGDP. The payment schedule shall be made under the following terms and conditions:

a. **Payment for Hardware and Software.**

(1) **Milestone-1 (Survey for Design and Drawing of BNNET-P1).** 10% price of Passive hardware value and 10% of Active Hardware value shall be paid after signing the contract and upon submission of the followings:

(a) A “Tier-III Certified Design and Layout Approval Certificate for Central Data Center” by UPTIME INSTITUTE (USA) or equivalent org and accepted by PURCHASER (BNTM Committee).

(b) A “Survey and Design Layout Completion Certificate” by the PURCHASER that the Survey report with design, drawing and Installation layout of BNNET-P1 submitted by the BIDDER/SUPPLIER and accepted by PURCHASER (BNTM Committee).

(c) Bank Guarantee (BG) for the 10% of the total active and 10% of total passive hardware price.

(d) Commercial Invoice signed by the supplier .

(2) **Milestone-2 (Receiving of Passive Hardware Items).** 40% price of Passive hardware item shall be paid on submission of followings:

(a) “BNNET-P1 Infrastructure Development Completion Certificate” by PURCHASER (BNTM Committee).

(b) “Certificate of Receiving LOT Passive Item (To be mentioned by the Bidder)” at designated BN site with FAT acceptance certificate and endorsed by the PURCHASER (BNTM Committee).

(c) Warranty/ Guarantee Certificate by the Manufacturer/ Supplier.

(d) Commercial Invoice signed by the Supplier.

(3) **Milestone-3 (Setting-to-Work of Passive Hardware Items).** 30% price of Passive hardware items shall be paid on submission of followings:

(a) “BNNET-P1 Fiber Optics Cable Laying Completion Certificate” by the PURCHASER (BNTM Committee).

(b) “BNNET-P1 Structure Cabling Completion Certificate” by the PURCHASER (BNTM Committee).

(c) “CDC and DRDC- Power Supply Arrangement Setting-to-Work Completion Certificate” by the PURCHASER (BNTM Committee).

RESTRICTED

(d) “CDC and DRDC- Air Condition Setting-to-Work Completion Certificate” by the PURCHASER (BNTM Committee).

(e) Commercial Invoice signed by Supplier.

(4) **Milestone-4 (Receiving of Active Hardware Items)**. 50% of Active Hardware value shall be paid on submission of followings:

(a) “Certificate of Receiving all Active Hardware Items (To be mentioned by the Bidder)” at designated BN site with FAT acceptance certificate and endorsed by the PURCHASER (BNTM Committee).

(b) “Certificate of Receiving Workstation PC” at designated BN site with acceptance certificate from CINS (BN) and endorsed by the PURCHASER (BNTM Committee).

(c) Warranty/Guarantee Certificate by Manufacturer/ Supplier.

(d) Commercial Invoice signed by Supplier.

(5) **Milestone-5 (Payment for Software Service)**. 80% (eighty percent) price of the total software value shall be released upon submission of the followings:

(a) “Subscription Certificate of BNNET-P1’s Software” and accepted by the PURCHASER (BNTM Committee).

(b) "Setting-to-Work Certificate of BNNET-P1’s Software" and accepted by the PURCHASER (BNTM Committee).

b. **Payment for Training and Technical Services.**

(1) **Milestone-6 (Payment for Foreign Training)**. 100% cost of foreign training shall be paid on submission of "Foreign Training Completion Certificate" issued by the PURCHASER (BNTM Committee)).

(2) **Milestone-7 (Payment for Local Training)**. 100% cost of local training shall be paid on submission of "Local Training Completion Certificate" issued by the PURCHASER (BNTM Committee).

(3) **Milestone-8 (Payment for Installation and Trial Run)**. 100% cost of Installation, Integration with VSAT link (if installed and run) and Trial-run shall be paid on successful completion of commissioning of BNNET-P1 and on production of "Job Completion Certificate" issued by the PURCHASER (BNTM Committee).

c. **Final Acceptance and After Sales Support Service.**

(1) **Milestone-9 (Final Acceptance of BNNET-P1)**. 20% of Passive Hardware value, 40% of Active Hardware item value and 20% of software service value shall be released upon submission of followings:

RESTRICTED

(a) "Tier-III Certification from Uptime Institute (USA)/ equivalent org for CDC" and accepted by the PURCHASER (BNTM Committee) for releasing last 20% of passive hardware value of CDC only.

(b) "Final Acceptance Certificate of Spare,Tools and Test Equipment" by the PURCHASER (BNTM Committee).

(c) "Final Acceptance Certificate of the BNNET-P1" by the PURCHASER (BNTM Committee).

(d) Submission of Warranty for Guarantee in the form of Bank Guarantee (BG) for an amount equivalent to 5% (five percent) of Total Contract Price (TCP) . This BG shall remain in vogue, which shall be released on receipt of 'No Objection Certificate' from the PURCHASER (BN) after the warranty period.

(e) Commercial Invoice signed by supplier.

(2) **Milestone-10 (After Sale Technical Support Service)**. 100% cost of 'after sale technical support service' shall be paid (if availed) on successful completion of service as stated in tender and on production of "Job Completion Certificate" issued by the PURCHASER (BNTM Committee).

d. **Milestone-11 (Data Center Tier-III Certification Service)**. 100% cost of Tier-III Certification Service shall be paid on submission of "Tier-III Certification Service Completion Certificate" issued by the PURCHASER(BNTM Committee).

e. **Part/Partial Payment**. Part/Partial Payment shall be allowed as per terms of payment stated in article 118.

119. **Price Escalation**. Total contract value shall not be escalated after the contract sign due to any reason.

120. **Price Details**. The price quotation shall include local TAX, VAT and other charges as applicable as per the existing govt rules of Bangladesh. The bidder shall offer the price quotation of all supplied items and services as per following format:

Ser	Description	Qty (Set)	Unit Price (BDT)	Total Price (BDT)
<u>Cost for Active Hardware</u>				
1.	CDC (Active Equipment for Data Center)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
2.	DRDC (Active Equipment for Data Centre)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
3.	NHQ DC (Active Equipment for Data Center)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
4.	UDC (Active Equipment for Data Center/Network Room of Command HQ & Base)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
5.	Ship (Active Equipment for Network Room)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer

RESTRICTED

Ser	Description	Qty (Set)	Unit Price (BDT)	Total Price (BDT)
6.	Workstation PC (End User)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
7.	Printer & Scanner	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
8.	Ancillary Equipment (CDC, DRDC, NHQ DC, Base and Ship)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
9.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Software</u>				
10.	CDC (Software for CDC, DRDC, NHQ DC, UDCs NOC, SOC Management and End User PC)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
11.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Passive Hardware</u>				
12.	Passive Hardware for CDC	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
13.	Passive Hardware for DRDC	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
14.	Passive Hardware for NHQ DC	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
15.	Passive Hardware for UDC (Command HQ & Base)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
16.	Passive Hardware for UDC(Ship)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
17.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Infrastructure Development Work</u>				
18.	Works for DC	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
19.	Furniture's for CDC, DRDC, NHQ DC and UDC (Command HQ, Base and Ship)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
20.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Cable Laying</u>				
21.	Cabling of Fiber & UTP (CDC, DRDC & NHQ DC)			

RESTRICTED

Ser	Description	Qty (Set)	Unit Price (BDT)	Total Price (BDT)
	a. Cost of UTP Cables	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	b. Cost of UTP cable Laying Service	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	c. Cost of Fiber Cables	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	d. Cost of Fiber cable Laying Service	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
22..	Cabling of Fiber & UTP (All UDCs of Command HQ & Base)			
	a. Cost of UTP Cables	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	b. Cost of UTP cable Laying Service	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	c. Cost of Fiber Cables	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	d. Cost of Fiber cable Laying Service	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
23.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Spares and Tools</u>				
24.	Tools and Test equipment	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
25.	Spares	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
26.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Data Link Service</u>				
27.	Data Link (NTTN) (One time Cost)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
28.	Yearly Recurring Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
29.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Training Package</u>				
30.	Foreign Training Package			
	a. Training Cost (Tuition Fee)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
	b. Admin Assistance (Air Fare, Boarding, Lodging and Local Transport)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer

RESTRICTED

Ser	Description	Qty (Set)	Unit Price (BDT)	Total Price (BDT)
31.	Local Training Package	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
32.	Misc Cost	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Installation and acceptance service</u>				
33.	Installation and Acceptance	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
34.	Inspections (FAT and PSI)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
35.	Any other cost (if any)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Data Center Tier-III Certification Service</u>				
36.	Design validation: Tier-3 from Uptime Institute USA/epi	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
37.	Data Center Certification: Tier-3 from Uptime Institute USA/epi	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
38.	Any other cost related to Tier certification	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Maintenance Service</u>				
39.	Maintenance Support Service (05 Years after the final acceptance)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
40.	Any other cost (if any)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
<u>Cost for Optional Items and Services</u>				
41.	Optional Items (As mentioned in various articles of tender spec)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
42.	Optional Services (As mentioned in various articles of tender spec)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
43.	Any other cost (if any)	As per BOQ	To be mentioned in Financial Offer	To be mentioned in Financial Offer
Grand Total =				

Item stated in the "Bill of Quantity" is given in Annex N "Bill of Quantity"

NOTE:

- Item wise price along with Qty and Unit price are to be submitted as per the Bill of Quantity and as stated in the tender requirement separately.
- Purchaser may select or discard any item considering the it's immediate requirement or operational need .

3. Lowest bidder shall be determined based on Grand Total value (i.e price of Mandatory items plus optional items).

121. **Insurances.** All insurance charges for hardware or material package shall be arranged and paid by the Bidder.

122. **Custom Duty and Taxes.** The hardware and software of BNNET-P1 shall, in general, be considered as 'Defense Stores' in Bangladesh. These defense stores shall be used only by the Defense Forces of Bangladesh and hence may be exempted from payment of custom duties and sales taxes in Bangladesh (for exempted items only) as per the Government of the People's Republic of Bangladesh, Ministry of Finance, National Bureau of Revenue (NBR) Memo No 9 (41) NBR/Cus-IV/72/246 dated 10 Apr 1981 and Government amendment.

123. **Vendors' List and User List of BNNET-P1 System.** Vendor list with Full address of the Vendors including fax number and e-mail address is to be provided for all vendor item used in BNNET-P1 and its associated equipment.

124. **Certificate to be Provided.** Following certificates are to be provided by the SUPPLIER along with equipment and the system:

- a. Authenticity Certificate from each vendor item stating that items are supplied from genuine source, brand new and year of manufacture.
- b. A Certificate of Assurance to the effect that the same/ similar hardware, software, and software license will be available for next 10 years.
- c. Service support for 24/7 (both principal and local agent) assurance certificate.
- d. Licensing certificates for applicable hardware, software, and software license.
- e. Software update service assurance certificate.
- f. Certificate on setting up of local office.
- g. Warranty/ Guarantee Certificate.
- h. Any other certificate which is not mentioned above, but required for the smooth functioning of the system must be given.

125. **Site Survey by Bidder.** The Bidder shall conduct a pre-bid/ post-bid (if contract is awarded) site survey by its expert team in all designated sites (Dhaka, Chattogram, Khulna area). The comprehensive site survey report shall be submitted with offer mentioning the location (Lat and Long), Room dimensions, Floor Height, Nearest MDB Box with cable laying distance, existing setup (i.e network hardware and ancillary equipment if any), Generator connection and shed and building protection system etc.

126. **Work Plan.** The Bidder shall submit the preliminary work plan with the offer. However, the bidder shall submit the final work plan of entire project works (12 months) within four weeks of signing the contract which will contain detailed information (Day, week and month) of all activities.

127. **Validity of Offer.** The offer will remain valid for 08 (Eight) months from the date of submission of the tender.

ANNEXES:

- A. Active Hardware- CDC DRDC & Network Room
- B. Software – CDC DRDC and PC
- C. Passive Hardware CDC DHAKA
- D. Passive Hardware DRDC CTG, NHQ DC & UDCs
- E. Genset & Substation CDC
- F. Genset & Substation DRDC
- G. Infrastructure Development Works - CDC
- H. Infrastructure Development Works – DRDC
- J. Cabling Works -Fiber & UTP Cabling
- K. Data Link – NTTN
- L. Tools and Test Equipment
- M. Training Package- Foreign and Local
- N. Bill of Quantity - Overall

**TECHNICAL SPECIFICATION OF ACTIVE HARDWARE - CDC, DRDC, NHQ
DC, UDC (Command HQ, Base & Ships)**

Technical Specification of Servers

1. Rack Server Type 1		
Items	Required Technical Specifications	Bidder's Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Integration requirement	All the hardware components (Server & Switch) should be from same OEM	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Manufacturing Country	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
Form factor	2U Rack Mountable Server	
Processors	Each server should have Two (02) numbers of latest 5th Generation Intel I5416S (2 GHz / 16-Core/ 30MB Cache) Processor from day-1	
Memory	Should have at least 32 DIMM slots per server and support minimum up to 8TB of DDR5 memory.	
	Should be proposed with minimum 256GB of DDR5 Memory using min.32GB RDIMM	
	Support for advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring.	
Storage	Server should be provided with	
	6 x 480GB 2.5inch Enterprise Value SSD Drive	
	RAID controller should support RAID 0, 1, 5, 6, 10, 50, and 60 minimum RAID Controller 4GB of Flash backed write cache module (FBWC).	
Network	Should be provided with Min. 2 * Dual-port 32G FC HBA	
	Should be provided with Min. 2 * Quad-port 10G/25G SFP+ NIC .	
	Should be provided with Min.1-Gbps RJ-45 Management port.	
PCIe Slots	Should support up to Up to 8 x PCIe Gen 4.0 slots or up to 4 x PCIe Gen 5.0 slots.	
Security and Other Features	Should support Hardware Policy based security	
	Should support anti-counterfeit measures to guarantee authenticity	
	The proposed solution should use AI/ML technology for infrastructure firmware updates & upgrades for the proposed system.	
	Should include TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, module from day-1	
	Should support Redfish Version 1.13.0	

RESTRICTED

	Should support Intelligent Platform Management Interface (IPMI) v2.0	
	Should support Simple Network Management Protocol (SNMP) v2 and v3	
	Should support Key Management Interoperability Protocol (KMIP)	
	Should support cKVM, Syslog, XML API	
	Should support Command-line interface (CLI)	
	Should support Secure Debug BIOS and BMC Comms	
Unified monitoring and management	Should support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring and reporting. Zero-touch auto configuration to auto deploy a baseline server configuration profile Automated hardware configuration and Operating System deployment to multiple servers	
	Should support industry standard management protocols like IPMI v2 and SNMP v3. The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure. With option to create unique dashboards for individual users. The user should have flexibility to select names for dashboards and widgets ex: - health, utilization etc.	
	The management solution must able to provide single console for managing all associated components like Servers, raid settings, NIC/HBA cards, Power supplies, Fans. Licenses to support the features to be supplied for fully populated chassis.	
	Solution should provide Centralized and embedded management with seamless high availability built into the infrastructure. All Management modules should be redundant on day 1. Management modules should not be isolated to a single chassis. If that is the case, the modules should have redundancy in each chassis.	
	Proposed solution should be a Software-as-a-Service (SaaS) hybrid cloud operations platform which should deliver intelligent automation, observability, and optimization for traditional and cloud-native applications and infrastructure.	
	This unified solution should Simplify servers, Hyperconverged Infrastructures, and Network Insights with 3rd Party Storage like- NetApp, Pure, and Hitachi storage management from a single management platform.	
	Should support for Configuration, provisioning, and installation with Policy-based profiles and templates for deployment, configuration, and the creation of multiple server profiles enable you to consistently deploy and configure servers, eliminating configuration errors and minimizing configuration drift. Should be capable to Install vMedia-based operating systems on the managed servers.	
	Solution should support templates to quickly make changes to the infrastructure. the server BIOS version, MAC ID, NIC firmware version, WWPN, FC-HBA firmware version, Adapter QoS , Management module firmware version, UUIDs , Server	

RESTRICTED

	Boot Policies, KVM IP etc. of the infrastructure required for workload	
	Should be able to provide Single Pane of Glass view management for both Rack Servers and Blade Servers together in a given location. The OEM has to offer their highest Management license. These licenses should be included on day 1.	
	Movement of server identity from one slot / server to another in the event of server failure. The movement of the identity should support both form factors of servers, that is blade to blade and rack to rack	
	Should be capable to Access on Android and iOS devices using a Mobile app providing a mobility-optimized connection to the resources managed in the account. That should help to stay up to date with the status of their environment and connect with members of the IT organization to address critical issues on the go. Also, should be able to Open TAC cases using this app and support multi-language.	
	The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure. With option to create unique dashboards for individual users. The user should have flexibility to select names for dashboards and widgets (ex:- health, utilization etc.)	
	Infrastructure Services SaaS/CVA - Essential licenses for 3 Years should be included in the solutions	
Power & Cooling	Must be provided redundant power supply and system fans from day-1.	
OS/ Virtualization Software	Should support Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, etc.	
OS License	OS License shall be provided as per the requirement stated in tender specification, article 32.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

RESTRICTED

2. Rack Server Type 2		
<u>Items</u>	<u>Required Technical Specifications</u>	<u>Bidder's Response</u>
Purpose	This server shall be used to run Active Directory services in the UDC mainly.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Integration requirement	All the hardware components (Routing, Switching, ESA, SMA & Server/HCI Node) should be from same OEM	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance.	
Integration requirement	All the hardware components (Server & Switch) should be from same OEM	
Environmental	Maintain International Quality Environmental Safety Standard	
Form factor	2U Rack Mountable Server	
Processors	Each server should have Two (02) numbers of latest 4th Generation Intel I4410T 2.7GHz/150W 10C/26.25MB DDR5 4000MT/s Processor day 1	
Memory	Should have at least 32 DIMM slots per server and support minimum up to 8TB of DDR5 memory.	
	Should be proposed with minimum 128 GB of DDR5 Memory using min.32GB RDIMM	
	Support for advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring.	
Internal Storage	Server should be provided with	
	5 x 960GB 2.5inch Enterprise Value SSD Drive from day 1 & up to 28 SFF drive for future scalability	
	RAID controller should support RAID 0, 1, 5, 6, 10, 50, and 60	
	minimum RAID Controller 4GB of Flash backed write cache module (FBWC).	
	Should be provided with Min. 1 * Quad-port 10G/25G SFP+ NIC .	
	Should be provided with Min. 1 * Quad-port 1G copper NIC	
	Should be provided with Min. 1 * Dual-port 16G/32G SFP+ FC ports to connect with SAN Switch.	
	Should be provided with Min.1-Dualps RJ-45 Management port.	
PCIe Slots	Should support up to Up to 8 x PCIe Gen 4.0 slots or up to 4 x PCIe Gen 5.0 slots.	
	Should support Hardware Policy based security	

RESTRICTED

Security and Other Features	Should support anti-counterfeit measures to guarantee authenticity	
	The proposed solution should use AI/ML technology for infrastructure firmware updates & upgrades for the proposed system.	
	Should include TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, module from day-1	
	Should support Redfish Version 1.13.0	
	Should support Intelligent Platform Management Interface (IPMI) v2.0	
	Should support Simple Network Management Protocol (SNMP) v2 and v3	
	Should support Key Management Interoperability Protocol (KMIP)	
	Should support cKVM, Syslog, XML API	
	Should support Command-line interface (CLI)	
	Should support Secure Debug BIOS and BMC Comms	
Unified monitoring and management	Should support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring and reporting. Zero-touch auto configuration to auto deploy a baseline server configuration profile Automated hardware configuration and Operating System deployment to multiple servers	
	Should support industry standard management protocols like IPMI v2 and SNMP v3. The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure. With option to create unique dashboards for individual users. The user should have flexibility to select names for dashboards and widgets ex: - health, utilization etc.	
	The management solution must able to provide single console for managing all associated components like Servers, raid settings, NIC/HBA cards, Power supplies, Fans. Licenses to support the features to be supplied for fully populated chassis.	
	Solution should provide Centralized and embedded management with seamless high availability built into the infrastructure. All Management modules should be redundant on day 1. Management modules should not be isolated to a single chassis. If that is the case, the modules should have redundancy in each chassis.	
	Proposed solution should be a Software-as-a-Service (SaaS) hybrid cloud operations platform which should deliver intelligent automation, observability, and optimization for traditional and cloud-native applications and infrastructure.	
	This unified solution should Simplify servers, Hyperconverged Infrastructures, and Network Insights with 3rd Party Storage like- NetApp, Pure, and Hitachi storage management from a single management platform.	

RESTRICTED

	Should support for Configuration, provisioning, and installation with Policy-based profiles and templates for deployment, configuration, and the creation of multiple server profiles enable you to consistently deploy and configure servers, eliminating configuration errors and minimizing configuration drift. Should be capable to Install vMedia-based operating systems on the managed servers.	
	Solution should support templates to quickly make changes to the infrastructure. the server BIOS version, MAC ID, NIC firmware version, WWPN, FC-HBA firmware version, Adapter QoS , Management module firmware version, UUIDs , Server Boot Policies, KVM IP etc. of the infrastructure required for workload	
	Should be able to provide Single Pane of Glass view management for both Rack Servers and Blade Servers together in a given location. The OEM has to offer their highest Management license. These licenses should be included on day 1.	
	Movement of server identity from one slot / server to another in the event of server failure. The movement of the identity should support both form factors of servers, that is blade to blade and rack to rack	
	Should be capable to Access on Android and iOS devices using a Mobile app providing a mobility-optimized connection to the resources managed in the account. That should help to stay up to date with the status of their environment and connect with members of the IT organization to address critical issues on the go. Also, should be able to Open TAC cases using this app and support multi-language.	
	The proposed solution should have customizable dashboard to show overall faults / health / inventory for all managed infrastructure. With option to create unique dashboards for individual users. The user should have flexibility to select names for dashboards and widgets (ex:- health, utilization etc.)	
	Infrastructure Services SaaS/CVA - Essential licenses for 3 Years should be included in the solutions	
Power & Cooling	Must be provided redundant power supply and system fans from day-1.	
OS/ Virtualization Software	Should support Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), VMware, etc.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned.	

RESTRICTED

	The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	
--	---	--

3. Hyperconverged Server		
Features	Required Specifications	Bidder's Response
Purpose	This server shall be used to run all the Data center management software and network device configuration as well as log keeping.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Integration requirement	All the hardware components (Routing, Switching, ESA, SMA & Server/HCI Node) should be from same OEM	
Hardware	Proposed Infrastructure Solution should come with fully redundant field replaceable components.	
Specifications	Proposed Infrastructure Solution should have independent hot swappable components which can be replaced and serviced without having the need to power down.	
	Proposed Infrastructure Solution should include x86 Nodes of following specifications.	
Computing and RAM Pool	Minimum 128 Physical Cores using Intel I5416S 2GHz/150W 16C/30MB DDR5 4400MT/s	
	Minimum 2 TB Memory using 64GB 4800MHz DDR5 RDIMM	
Storage Pool	Minimum 243 TB All flash capacity across the cluster using 7.6TB SSD drive.	
Boot Drive	Minimum 2 x 240GB M.2 Drive for booting with Boot optimized M.2 Raid controller	
Power Supplies and cooling fans	Redundant power supplies and system Fans.	
Network Interface	Should have minimum 2 x 4 Ports 10/25/50GB fiber NIC with SR Module.	
	Each adapter should support creation of at least 250 dynamic virtual adapters and interfaces without single-root I/O virtualization (SR-IOV) support from OSs or hypervisors with 10/25G CSR SFP28 module with Necessary FC cable	
Unified Switch	Bidder should includes min. Two (02) Quantity. of unified network switches (SAN/LAN Traffic), each with min. 36 ports per switch with redundant power supplies and cooling fans.	
	The switches should be provided with min. 36x10/25/40/100 Gbps or equivalent bandwidth for downlink ports and minimum 2*40Gb or 2* 100Gps Ethernet ports for uplink connectivity. All required SFPs/Active Optical Cables, licenses should be provided.]	
Hyper	The proposed solution should come with preinstalled various software including SDS with management and associated hypervisor. It should include all hardware and software	

RESTRICTED

	necessary to ensure high availability mode of operation. The proposed solution should have a Single Management Console to manage integrated Compute, Storage and Hypervisor. The solution must come with a bundle/customer license, which must be clearly mentioned in OEM's license portal. The platform and environment should be customizable as per the requirement of User. The proposed HCI solution should be able to leverage SSD not only for caching but for capacity also to optimized read IO's and there should not be any limitation on SSD overall caching on software defined storage. The proposed solution should be completely software defined and should not rely on any hardware RAID controller.	
Converged	The HCI solution should include Hypervisor License and should support minimum 3 of the industry leading hypervisors.	
Solution	Dashboard to manage and provision virtual machines, network, storage, monitor performance and manage events & alerts. It should also contain a dashboard for monitoring & generating reports. The solution should provide a log analytical tool which will show all the logs available in one single management console and a single location to collect, store, and analyze unstructured data from OS, apps, storage, network devices, etc. to make troubleshooting easier. Solution provider OEM should be able to provide the Virtualization software for Server.	
Requirements	Technology must be software defined and the solution should provide enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network & associated components such as SAN Switches & HBAs. The solution should have data locality.	
	The solution must be able to survive single node failures and it should in no way affect/degrade the production services & usable resources to the end user application. Solution must support all the mentioned industry Leading protocols NFS, iSCSI & SMB.	
	Solution should include an application and infrastructure performance management tool quoted as part of the solution to improve operations and provide deep infrastructure performance insight.	
	Proposed solution should cater virtualized core based licensing for products like (but not limited to) Oracle, MSSQL etc. The solution must natively support RDMA for better performance.	
	It should be possible to use different storage policies in the storage LUNs/Container with Storage QoS	
	Solution should support live migration of running virtual machines from one physical node to another with zero downtime and continuous service availability.	
	The solution should provide enterprise data services such as deduplication, encryption & compression without dependence on any proprietary hardware. This should be delivered in both all flash as well as hybrid solution. These functionalities should be part of the proposed solution and licensed. The proposed	

RESTRICTED

	HCI solution should be able to create multiple logical unit (LUN's) for storage with multiple policy for deduplication and compression across storage logical unit. The Proposed HCI solution should support Erasure Coding for archival data storage.	
	The proposed solution must support connectivity (Storage extension) to 3rd party bare metal servers (for optimized DB licensing on physical servers) to storage cluster & use the cluster capacity like (but not limited to) iSCSI, NFS target.	
	The proposed solution should support Hybrid and All Flash Nodes in the same cluster. Proposed SSD should be used for both storing Data and Caching. (If OEM uses SSD/NVMe dedicatedly for caching then additional SSD should be proposed). It should be possible to Pin IOPS hungry VMs on SSD only	
	Proposed solution should have inbuilt Data at Rest Encryption (DARE) and should also include a Key Management Solution. (OEM should not depend upon 3rd party key management solution or specific hardware to achieve the same)	
	The solution should support to connect external storage devices (like NAS, SAN etc.) and should be useable as part of the Solution, for the purpose of Backup. There should not be any hardware vendor locking while connecting the external storage/s and this can be accessed over IP (No proprietary protocol should be used).	
Scalability	Proposed solution shall support unlimited nodes in a same cluster without any federation	
	The solution should be able to scale by support of adding additional nodes to the cluster at a later point of time to handle compute, Memory & Storage requirements. Solution should support cluster expansion with zero down time. The proposed solution should support hybrid and all flash nodes in same cluster for future scalability. HCI solution must have capability to support HCI nodes with different models, different CPU Generations & Memory, Disks configurations in the same cluster without any impact on enterprise class storage services/functionalities	
	Data compression, deduplication, erasure coding techniques should be available with licenses (if applicable) in the Software Defined Storage (SDS) layer for use without additional cost.	
Data Protection	Ability to provide Replication of Virtual machine backup locally and in Disaster Recovery site. (VM level Mirroring) to protect selected VM's. If licensing module is there, bidder should provide licensing details. Should come with solution and should implement from Day 1 of operation.	
	Solution should be able to take App and database consistent snapshot and should be able to schedule the same.	
	Shall be able to restore VM from the backup.	
Remote	HCI solution should support file level recovery of user's data from VM's without Storage/VM's admin involvement	

RESTRICTED

Replication	HCI solution should support unlimited VM's snapshot at storage level, it should not impact guest OS performance during snapshot.	
	HCI solution should be able to take VM's snapshot/Storage snapshot at any time irrespective of VM's state (Power ON/Power OFF/Suspended) with retention policy	
	HCI solution should support crash consistent and application consistent backup within cluster	
	HCI solution should support VM's backup on leading cloud providers, AWS, GCP, Azure	
	HCI solution must support two copies of data across cluster and should have capability for supporting three copies for critical data and it should be available on workload level.	
	HCI solution should support data replication across sites with customized RPO i.e. 0 mins/5 mins/15 mins and grouping of Virtual machine as per application architecture	
	HCI solution should support WAN Bandwidth optimizer along with defined schedule across two sites and only increment data should be replicated post one time data sync	
	HCI solution should have license for three way DR for active-active configuration on MetroCluster, near sync, async replication with defined RPO, some of VM's are working from Primary (Site-A) and their DR at DR sites (Site-B) and Some of the VM's are working from Site-B and their DR's is at Site-A. It should have feature to change VM IP's on the fly without manual intervention in case the DR site has different subnet from DC Site. The Replication software should provide DR Orchestration and should be able to do VM power up sequencing. License should be provided for unlimited VMs	
Hypervisor	The solution shall provide a purpose-built hypervisor with minimal footprint that installs directly on the 64 bit bare metal x86 dual socket servers	
	Hypervisor should support container and openstack integration for cloud native application	
	Virtualization Manager should have integrated Physical Host/ Node and Virtual Machine performance monitoring with high availability construct. No single point of failure for Virtualization Manager	
	Single view of all virtual machines, allow Monitoring of system availability and performance and automated notifications with alerts. Monitor, analyze virtual machines, server utilization availability with detailed performance graphs and greater visibility into object relationships	
	High Availability capabilities for the VMs in the sense if in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server / node running same virtualization software	
	Ability to thin provision disks to avoid allocating all storage space upfront. Full monitoring capabilities & alerts to prevent from accidentally running out of physical storage space should be there	

RESTRICTED

	Hypervisor should support virtualization guest tools inside guest for optimized performance for video/network/performance and disk reclaim options from guest OS's	
	Hypervisor should support OVA/OVF image import and export	
	Hypervisor must have capability for OS Catalogue/template and OS provisioning with role-based access to virtual machine	
	Capability for creating Virtual machine templates to provision new servers and also allow taking point in time snapshots of the virtual machines to be able to revert back to an older state if required	
	Hypervisor should have integrated snapshot-based backup, schedule backup/restore and configure multiple copies of backup on periodic interval	
	Proposed hypervisor should support standard features like nondisruptive migration of workload across hosts, High Availability and Distributed resource scheduling during resource constrain	
	Hypervisor shall provide automated live migration for initial placement and balancing of available resources with the rules to define affinity and / or antiaffinity of workloads	
	Hypervisor solution must allow seamless migration across different CPUs with Enhanced Compatibility mode per-VM during migrations across hosts in a clusters and during power cycles	
	Hypervisor shall provide the ability to hot add CPU and memory, hotplug disks and NICs (provided the same is supported by guest OS	
	Hypervisor should provide ability to grant / ensure resources to virtual machines as they need for hosting critical workloads. Also the initial placement of workloads should consider CPU, Memory and Storage contentions / hotspots	
	Hypervisor shall provide zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process	
	Hypervisor should support UEFI bios along with legacy BIOS for supported virtual guests OS	
	Virtualization Manager should automatically check cluster components, hosts, storage, network, hardware and cause of performance issue on configurable schedule with results on designated email.	
	Virtualization Manager should be able to identify out of the box top 10 VM's basis on their high resource utilization (CPU/ Mem/ Storage/ Network) on single dashboard	
	Virtualization Manager must support Directory based/OpenLDAP and SAML based authorization for management	
	Virtualization manager should keep at least 90 days historical performance data for VM's/Storage and partnering host	

RESTRICTED

	Hypervisor/management must should be able to disable SSH based login to cluster for security and should have support for ssh key based login	
	Hypervisor and Management must support SNMP version 3 and SMTP for proactive alerting and email configuration	
	Hypervisor must provide centralized interface from which virtual machine access switching for the entire virtual datacentre can be configured , monitored and administered	
	The Virtualization manager should provide a virtual switch which can span across a virtual datacentre and multiple hosts should be able to connect to it. This in turn will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches	
	Virtualization Manager should provide feature which can perform quick, asneeded deployment of additional virtualized hosts. When the service is running, it can push out update images, eliminating patching and update without impacting production	
	3rd party support for endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions	
	Hypervisor should support Rest API and Command line management along with GUI interface.	
	Required Hypervisor License and Hypervisor Management should be included into the solution	
HCI Management	HCI solution should support automated and zero touch upgrades from single management pane/console for hardware/storage/hypervisor with no major impact on production	
	HCI solution should provide all key operation management and performance management from a single console for Hardware/ Storage /Hypervisor and VM 's management using HTML 5 internet browser	
	HCI solution management pane should integrated with Active Directory /LDAP	
	HCI solution must support monitoring via SNMPv3 and email alerting via SMTP	
	HCI solution should have analytics on capacity behaviour and should have capability of showing all under and over utilized VM's with their right sizing information after current VM's usages	
	HCI solution should be capable of creating custom dashboard with reporting as per customer ease and requirements, solution should be able to scan/search objects with advanced search option for faster access to require information for troubleshooting	
	HCI solution should have capability for finding object anomalies from standard behaviours and report this before major bottleneck for solution	

RESTRICTED

	HCI solution should have codeless automation native engine to create troubleshooting for alert and remediation as per policy	
	HCI solution should have capability for managing multiple sites/clusters from one HTML5 based browser with single sign on	
	HCI solution should support rest API for third party integration and customized workflow for automation using rest API	
	HCI solution should have call home capability for remote log collection and proactive support for predictive failure hardware component	
	HCI solution should provide seamless upgrade for Firmware, Hypervisor, Storage OS, BIOS and other such functions which are required in the HCI platform. The upgrade should be online and should not be done from one single pane of management	
	Offered solution should have inbuilt analysis for VMs and should be able to give report of VM performance for minimum 90 days. It should be possible to view constraint and overprovisioned VM from single GUI, it should be possible to create Customized Dashboard as per requirement.	
Private Cloud Orchestrator	The solution should have catalogue of private cloud services, and should support self-service provisioning capabilities	
	The solution should provide authentication, authorization and accounting (AAA) out of the box	
	The solution should have Life Cycle Management Work flows: Provisioning	
	Central administrator must be able to manage/control the marketplace view for the tenants. Any authorised user must be able to deploy the application using the published VMs in his application marketplace.	
	The solution should provide capability of generating reports for usage & performance	
	Ability to integrate with industry standard authentication like AD etc.	
	The model should include at least three user levels for the Platform (Admin/User/Monitor)	
	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network, storage through a unified multitenant IT service catalogue	
	The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific cloud and IT resources, while ensuring compliance with business policies	
	The solution must be able to provision VM's on ESXi or AHV hypervisor	
	The solution must allow restriction of vCPU, Memory and Disk resources to each project or group of users	
The solution must allow management of existing/already provisioned VMs and perform automation task		

RESTRICTED

	The solution must provide full audit governance on who launch the blueprint, output log of each action and script used to run the action	
	The solution must allow/support disk image of Windows, Windows Server, all variant of Linux.	
	The solution must allow single management console to view the capacity, performance of the infrastructure and the blueprint designer without logging in to different url.	
	The solution must support HTML5	
	The solution must provide a marketplace to allow user to consume the creation of infrastructure easily	
	The designer can define the vCPU & memory for each virtual machine	
	The designer can define the vCPU & memory for each virtual machine	
	The software must be able to integrate with monitoring software.	
	The software must be able to integrate with application security vulnerabilities detection software The Software should have user management capabilities to support the following:	
	a) Highly configurable user role model	
	b) Mass maintenance of a group of users	
	The Software should support AD authentication, and synchronization of user list and profiles between Software and Active Directory setup.	
	The solution must provide machine intelligence to continuously provide optimization recommendations. Operator should be able to easily fix security vulnerabilities and right-size resources with just one-click. The solution should provide 250+ audit checks to ensure compliance with industry standard regulatory policies and best practices are met.	
	The application must be able to support separation of account creation and role assignment.	
	The application must be able to support Inactive session auto logout.	
Firmware Code and Patch Management	The solution should provide seamless upgrade for (but not limited to) Firmware, Hypervisor, Storage OS, SDS software, BIOS and other such functions which are required in the solution.	
	All patches for the complete hardware and software solution must come from a single validated source. It should be possible to apply and upgrade all software and Hardware related firmware and patches from the same GUI that is used to manage the HCI (It should not use the hardware management console for doing firmware upgrade of hardware)	
Proactive Maintenance and Support	Proposed Appliance should come with a single proactive incident reporting and alerting which covers both Hardware components and full Software stack.	
	Proposed solution should have one window support solution for all the components including hardware, firmware and software used. The support should be from OEM.	

RESTRICTED

	The OEM must have local office & Depot in Bangladesh and 24x7x365 Global TAC support along with Toll Free number should be available.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

Technical Specification Router

4. Core Router		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in Data Centers to communicate with the ISP router who will provide the internet service.	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 1 RU	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Router Processor Type	High-performance multi-core processors	
General / Functional Requirement	WAN architecture should have centralized control plane architecture.	
	It should provide transport layer independence and will allow to use any transport like MPLS, internet, point to point links between locations.	
	It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh.	

RESTRICTED

	WAN controllers should provide key wan capabilities like WAN edge device authentication on wan network, secure control communication with edge device, building overlay network as per requirement like hub & spoke, full mesh etc., best path computation, link performance computation based on latency, loss and jitter, traffic load balancing on secure overlay network based on policy, build and apply various policies and control from central locations like change in topology, applying ACL, QoS, centralize monitoring and management.	
	WAN edge device should perform actual data forwarding based on control communication from centralize controller.	
	It should build secure IPsec network between locations for secure communication and allow various last mile connectivity."	
DRAM	Min. 16GB (installed) Max 64 GB Upgradable	
Hardware Capacity	Router should support in SD-WAN mode min. 90 Gb and Non-SD-WAN mode forwarding throughput min.195 Gbs from day 1 in 1400 bytes.	
Flash Memory	Default min. 32-GB eUSB flash storage	
Power Supply	Redundant power Supply from day 1	
Interfaces	Router should have <ul style="list-style-type: none"> • Min. 12-port 1/10GE , • 2 x 40GE , • 2 x 40/100GE ports. Bidder has to provide <ul style="list-style-type: none"> • 8 x 10G short range optical transceiver & • 4 x 40G short range optical transceiver with each devices from Day 1. All the modules are OEM original and same as "Router" brand	
	Management: 1 x console and 1 x Gigabit Ethernet port for device management	
	USB: 2 x USB 2.0 Type A port. Serial: 1 x auxiliary port	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security:	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
	Should have up to 130 Gbps of IPsec Internet Mix (IMIX) traffic in Non SDWAN mode 3900 tunnels. Router should have support at least 3.5M IPV4 and IPV6 route from day 1. Number of ACL 3900, Number of Firewall session 5.9M, VRF 7900 from day 1, No of NAT session 5.9M.	
	Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.	
	WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point.	

RESTRICTED

	It should be possible to create minimum 4 segments from day-1.	
	Should support ACL for IPv4 and IPv6, Time based ACL,	
	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers	
	like Amazon and Azure and they should able to connect on WAN like any other branch location"	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Management	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

RESTRICTED

Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	
--------------------------------	--	--

5. Internet/DMZ Router		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in Data Centers to communicate with all the routers in different Command HQ, Base and Ships	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 1 RU	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Router Processor Type	High-performance multi-core processors	
General / Functional Requirement	WAN architecture should have centralized control plane architecture.	
	It should provide transport layer independence and will allow to use any transport like MPLS, internet, point to point links between locations.	
	It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh.	
	WAN controllers should provide key wan capabilities like WAN edge device authentication on wan network, secure control communication with edge device, building overlay network as per requirement like hub & spoke, full mesh etc., best path computation, link performance computation based on latency, loss and jitter, traffic load balancing on secure overlay network based on policy, build and apply various policies and control from central locations like change in topology, applying ACL, QoS, centralize monitoring and management.	

RESTRICTED

	WAN edge device should perform actual data forwarding based on control communication from centralize controller.	
	It should build secure IPsec network between locations for secure communication and allow various last mile connectivity."	
DRAM	Min. 16GB (installed) Max 64 GB Upgradable	
Hardware Capacity	Router should support in SD-WAN mode min. 19 Gb and Non-SD-WAN mode forwarding throughput min.38 Gbs from day 1 in 1400 bytes.	
Flash Memory	Default min. 32-GB eUSB flash storage	
Power Supply	Redundant power Supply from day 1	
Interfaces	<p>Router should have</p> <ul style="list-style-type: none"> • Min. 4-port 1/10GE & • 8-port 1GE ports. <p>Bidder has to provide</p> <ul style="list-style-type: none"> • 4 x 10G short range optical transceiver & • 4 x 1G short range optical transceiver with each devices from Day 1. <p>All the modules are OEM original and same as "Router" brand</p>	
	Management: 1 x console and 1 x Gigabit Ethernet port for device management	
	USB: 2 x USB 2.0 Type A port. Serial: 1 x auxiliary port	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security:	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
	Should have up to 19 Gbps of IPsec Internet Mix (IMIX) traffic in Non SDWAN mode 3900 tunnels. Router should have support at least 3.5M IPV4 and IPV6 route from day 1. Number of ACL 3900, Number of Firewall session 5.9M, VRF 7900 from day 1, No of NAT session 1.9M.	
	Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.	
	WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point.	
	It should be possible to create minimum 4 segments from day-1.	
	Should support ACL for IPv4 and IPv6, Time based ACL,	
	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers like Amazon and Azure and they should able to connect on WAN like any other branch location"	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate	

RESTRICTED

	System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Management	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

6. WAN Router		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in Data Centers to communicate with all the routers in different Command HQ, Base and Ships	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 1 RU	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Router Processor Type	High-performance multi-core processors	
General Functional Requirement /	WAN architecture should have centralized control plane architecture.	
	It should provide transport layer independence and will allow to use any transport like MPLS, internet, point to point links between locations.	
	It should build secure overlay network on any transport and will allow to create various topology like Hub & spoke, full mesh, partial mesh.	
	WAN controllers should provide key wan capabilities like WAN edge device authentication on wan network, secure control communication with edge device, building overlay network as per requirement like hub & spoke, full mesh etc., best path computation, link performance computation based on latency, loss and jitter, traffic load balancing on secure overlay network based on policy, build and apply various policies and control from central locations like change in topology, applying ACL, QoS, centralize monitoring and management.	
	WAN edge device should perform actual data forwarding based on control communication from centralize controller.	
	It should build secure IPsec network between locations for secure communication and allow various last mile connectivity."	

RESTRICTED

DRAM	Min. 16GB (installed) Max 64 GB Upgradable	
Hardware Capacity	Router should support in SD-WAN mode min. 19 Gb and Non-SD-WAN mode forwarding throughput min.38 Gbs from day 1 in 1400 bytes.	
Flash Memory	Default min. 32-GB eUSB flash storage	
Power Supply	Redundant power Supply from day 1	
Interfaces	<p>Router should have</p> <ul style="list-style-type: none"> • Min. 4-port 1/10GE & • 8-port 1GE ports. <p>Bidder has to provide</p> <ul style="list-style-type: none"> • 4 x 10G short range optical transceiver & • 4 x 1G short range optical transceiver with each devices from Day 1. <p>All the modules are OEM original and same as "Router" brand</p>	
	Management: 1 x console and 1 x Gigabit Ethernet port for device management	
	USB: 2 x USB 2.0 Type A port. Serial: 1 x auxiliary port	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security:	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
	Should have up to 19 Gbps of IPsec Internet Mix (IMIX) traffic in Non SDWAN mode 3900 tunnels. Router should have support at least 3.5M IPV4 and IPV6 route from day 1. Number of ACL 3900, Number of Firewall session 5.9M, VRF 7900 from day 1, No of NAT session 1.9M.	
	Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.	
	WAN should support end to end segmentation with different routing table per segment and it should be possible to create per segment topology on WAN like HUB & Spoke, full mesh, partial mesh, point to point.	
	It should be possible to create minimum 4 segments from day-1.	
	Should support ACL for IPv4 and IPv6, Time based ACL,	
	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers	
	like Amazon and Azure and they should able to connect on WAN like any other branch location"	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote	

RESTRICTED

	Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Management	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

6. Branch Router Type 1		
Item	Required Specification	Bidder Response
Purpose	This device shall be used in UDC (Command HQ, Base and Ships), to communicate with the Data Centers of BNNET.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 2 RU	
Router Processor Type	High-performance multi-core processors	
DRAM	Min. 16GB (installed) Max 32 GB Upgradable	
Hardware Capacity	Router should min.19 Gbps from day 1 in 1400 bytes.	
Flash Memory	Integrated Min. 8 GB (installed) Flash Memory	
Interfaces	Router should have <ul style="list-style-type: none"> • Min. 4x1GE WAN & • 8x1G L2 ports from day 1. Bidder has to provide 4 nos of 1G SFP module from day 1. All SFP should be from the same OEM.	
	USB: 2 x USB 2.0 Type A port. Serial: 1 x auxiliary port	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
	Should support Up to 2Gbps of IPsec Internet Mix (IMIX) traffic. Should support SDWAN mode & Non SDWAN mode 3900 tunnels. Router should have support IPv4 Routes 1.5 M and IPv6 Routes 1.4 M from day 1. Number of ACL 3900, Number of Firewall session 510K, VRF 3900 from day 1. Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.	
	Should support ACL for IPv4 and IPv6, Time based ACL,	

RESTRICTED

	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers like Amazon and Azure and they should be able to connect on WAN like any other branch location"	
Interface support	Support Gigabit Ethernet, T1/E1, Channelized E1/T1, FXO, 4G/LTE Service Card	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QoS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Expansion Slots	Should have min. 1 Service module & 1 NIM Module slots from day 1.	
High Availability	Support On-Line Insertion (OIR) for Network Interfaces Modules to reduce downtime during fault/repair/upgrade	
	Redundant power Supply from day 1	
Other Features	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details' part numbers and Manufacturer's Warranty letter.	

RESTRICTED

	Bidder must submit the required performance document and compliance reference document for the proposed device.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

6. Branch Router Type 2		
Item	Required Specification	Bidder Response
Purpose	This device shall be used in UDC (Command HQ, Base and Ships), to communicate with the Data Centers of BNNET.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 2 RU	
Router Processor Type	High-performance multi-core processors	
DRAM	Min. 8GB (installed) Max 32 GB Upgradable	
Hardware Capacity	Router should min.3.5 Gbps from day 1 in 1400 bytes.	
Flash Memory	Integrated Min. 8 GB (installed) Flash Memory	
Interfaces	Router should have <ul style="list-style-type: none"> • Min. 4x1GE WAN Bidder has to provide 2 nos of 1G SFP module from day 1. All SFP should be from the same OEM.	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	

RESTRICTED

	<p>Should support Up to 900 Mbps of IPsec Internet Mix (IMIX) traffic.</p> <p>Should support SDWAN mode & Non SDWAN mode 2400 tunnels.</p> <p>Router should have support IPv4 Routes 1.5 M and IPv6 Routes 1.4 M from day 1.</p> <p>Number of ACL 3900,</p> <p>Number of Firewall session 510K,</p> <p>VRF 3900 from day 1.</p> <p>Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.</p>	
	Should support ACL for IPv4 and IPv6, Time based ACL,	
	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers like Amazon and Azure and they should able to connect on WAN like any other branch location"	
Interface support	Support Gigabit Ethernet, T1/E1, Channelized E1/T1, FXO, 4G/LTE Service Card	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 802.3ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Expansion Slots	Should have min. 1 PIM & 1 NIM Module slots from day 1.	

RESTRICTED

High Availability	Support On-Line Insertion (OIR) for Network Interfaces Modules to reduce downtime during fault/repair/upgrade	
Other Features	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details' part numbers and Manufacturer's Warranty letter.	
	Bidder must submit the required performance document and compliance reference document for the proposed device.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

Technical Specification of Switch

7. WAN Switch		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in the Data centers (CDC, NHQDC and DRDC) for connecting the DMZ servers.	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack-mountable	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	

RESTRICTED

General Features	<ul style="list-style-type: none"> • The switch should have minimum 24 x 1/10/25G Ethernet and • 4 x 40/100GE uplink ports with • 12 x 1/10 GE short range optical transceiver, • 12 x 10/25 GE short range optical transceiver & • 4 x 40G short range optical transceiver modules with each devices from Day 1. • All the modules are OEM original and same as "Switch" brand 	
	Switch should have stacking feature	
	Should have minimum 16GB DRAM & 16GB Flash	
	Switch should have redundant power supply from day 1.	
Performance	Minimum Switching capacity min 2 Tbs	
	Minimum Forwarding Throughput min 1Tbs	
Layer-2 Features	Layer 2 switch ports and VLAN trunks	
	IEEE 802.1Q VLAN encapsulation	
	Support for up to 4000 VLANs ID	
	Minimum 82,000 MAC Address	
	Support minimum 9216 bytes Jumbo frame	
	Switch should have Layer 2, Routed Access (RIP, OSPF) PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-256 bit, CoPP, SXP, IP SLA Responder from day 1.	
	Must have 16 MB of shared buffer for traffic/packet Queuing and processing	
Layer-3 Feature	The Switch should support routing protocols such OSPF, BSR, IS-ISv4, LISP, VXLAN, VRF.	
	Support Routing protocols IS-IS, IP SLA, OSPFv3	
	Minimum Up to 255,000 IPv4 route and IPv6 route	
	Support minimum 4000 L3 VLAN Interfaces or Switched Virtual Interfaces	
	The Switch should support IP Multicast and PIM, PIM Sparse Mode & Source-Specific Multicast for Wired and Wireless Clients.	
	The Switch should support basic IP Unicast routing protocols (static, RIPv1 & RIPv2).	
	The Switch should support IPv6 & IPv4 Policy Based Routing (PBR)	
	Minimum 64,000 flow entries for security and traffic visibility.	
	Support Internet Group Management Protocol (IGMP), PIM Stub etc.	
	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port.	
Security features	Support 802.1X, Flexible Authentication, 802.1x Monitor Mode, and RADIUS Change of Authorization.	
	Support minimum 1600 ACL entries. Access switch must support power redundancy across all models, either internally or via external RPS.	

RESTRICTED

	Support L2 IEEE 802.1AE -256-bit security from day 1. Switch shall support MACSec on access and uplink ports.	
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard	
	Switch Should support Policy-based Automation & Assurance for Wired & Wireless features.	
	Support OS, Firmware/BIOS & patch authenticity as encrypted images to protect from unauthorized and modified/cracked images.	
	Support OS validation during booting to protect from threats.	
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.	
	Switch should support API Driven configuration and support Netconf and Rest conf using YANG data model. It should support automation tool like python	
	Switch should support Patch Management feature.	
	Switch should support port mirroring based on Inbound & outbound, mirroring based on ports, vlans, RSPAN, ERSPAN	
	The switch must have at least 335,000 hours Mean Time Between Failure (MTBF) for hardware reliability.	
Compliance & Reference	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available and accessible document.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

8. Distribution Switch		
Feature List	Feature Description	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack-mountable	

RESTRICTED

Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
General Features	The switch should have minimum <ul style="list-style-type: none"> • 24 x 1/10/25G Ethernet and • 4 x 40/100GE uplink ports with • 10 x 1/10 GE short range optical transceiver • 12 x 1/10 GE Long range optical transceiver & • 4 x 40G short range optical transceiver modules with each devices from Day 1 All the modules are OEM original and same as "Switch" brand	
	Switch should have stacking feature	
	Should have minimum 16GB DRAM & 16GB Flash	
	Switch should have redundant power supply from day 1.	
Performance	Minimum Switching capacity min 2 Tbs	
	Minimum Forwarding Throughput min 1Tbs	
Layer-2 Features	Layer 2 switch ports and VLAN trunks	
	IEEE 802.1Q VLAN encapsulation	
	Support for up to 4000 VLANs ID	
	Minimum 82,000 MAC Address	
	Support minimum 9216 bytes Jumbo frame	
	Switch should have Layer 2, Routed Access (RIP, OSPF) PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, QoS, FHS, 802.1X, MACsec-256 bit, CoPP, SXP, IP SLA Responder from day 1.	
	Must have 16 MB of shared buffer for traffic/packet Queuing and processing	
Layer-3 Feature	The Switch should support routing protocols such OSPF, BSR, IS-ISv4, LISP, VXLAN, VRF.	
	Support Routing protocols IS-IS, IP SLA, OSPFv3	
	Minimum Up to 255,000 IPv4 route and IPv6 route	
	Support minimum 4000 L3 VLAN Interfaces or Switched Virtual Interfaces	
	The Switch should support IP Multicast and PIM, PIM Sparse Mode & Source-Specific Multicast for Wired and Wireless Clients.	
	The Switch should support basic IP Unicast routing protocols (static, RIPv1 & RIPv2).	
	The Switch should support IPv6 & IPv4 Policy Based Routing (PBR)	
	Minimum 64,000 flow entries for security and traffic visibility.	
	Support Internet Group Management Protocol (IGMP), PIM Stub etc.	
	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling,	

RESTRICTED

	Committed Information Rate (CIR), and eight egress queues per port.	
Security features	Support 802.1X, Flexible Authentication, 802.1x Monitor Mode, and RADIUS Change of Authorization.	
	Support minimum 1600 ACL entries. Access switch must support power redundancy across all models, either internally or via external RPS.	
	Support L2 IEEE 802.1AE -256-bit security from day 1. Switch shall support MACSec on access and uplink ports.	
	Support Port Security, Dynamic ARP Inspection, and IP Source Guard	
	Switch Should support Policy-based Automation & Assurance for Wired & Wireless features.	
	Support OS, Firmware/BIOS & patch authenticity as encrypted images to protect from unauthorized and modified/cracked images.	
	Support OS validation during booting to protect from threats.	
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring.	
	Switch should support API Driven configuration and support Netconf and Restconf using YANG data model. It should support automation tool like python	
	Switch should support Patch Management feature.	
	Switch should support port mirroring based on Inbound & outbound, mirroring based on ports, vlans, RSPAN, ERSPAN	
	The switch must have at least 335,000 hours Mean Time Between Failure (MTBF) for hardware reliability.	
Compliance & Reference	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available and accessible document.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

9. FC / SAN Switch		
Item	Required Technical Specifications	Bidder's Response
Purpose	This device shall be used in the CDC, NHQDC and DRDC for	

RESTRICTED

	Connecting the required RACK servers to the central Storage.	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Manufacturing Country	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
Form factor	Rack mountable and maximum 2U	
Architecture	Each SAN Switch shall be configured with minimum 24 Ports and scalable to 32 ports.	
	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.	
	Switch should have LED indicators for active system components like FAN, PSU, Ethernet ports, FC Ports, management ports, Chassis status, etc.	
Number of Ports	32 x 32Gb SW SFP ports with required transceivers from day-1	
FC Cables	08 numbers of minimum 25m LC-LC Cables 08 numbers of minimum 35m LC-LC Cables 08 numbers of minimum 45m LC-LC Cables 08 numbers of minimum 55m LC-LC Cables	
Performance	32 Gbps speed on all ports in an energy efficient fashion (Non-blocking architecture with 1:1 performance) with auto-sensing of 8/16/32 Gbps	
	Aggregate bandwidth of 1024 Gbps end-to-end full duplex	
	Up to 8300 for a group of 16 ports, with a default of 500 buffer credits per port and a maximum of 8270 buffer credits for a single port in the group	
	Up to 16 load-balanced physical links grouped in one port channel	
	The switch shall support different port types such as F-port & E-Port.	
Management & Other features	Switch should support Analytics for NVMe based fabric	
	Switch should include Analytics capability and traffic visibility for any ports at any time.	
	Switch shall have support for web-based management and should also support CLI	
	The switch should have USB port for firmware download, support save, and configuration upload/download.	
	Switch shall provide POST and online/offline diagnostics, Fcping and Pathinfo (FC Traceroute), Port mirroring (SPAN Port), Internal loopbacks, Syslog, FC debug, online system health, tricolour LEDs for Switch level component status.	

RESTRICTED

	Offered SAN Switch shall support services such as Quality of Service (QoS) to help optimize application performance, Inter-VSAN Routing (IVR), Logical Unit Number (LUN) zoning, VSAN-based access control. It should be possible to define high, medium and low priority QoS Zones to expedite high-priority traffic.	
	SAN switch shall support to restrict data flows from less critical hosts at preset bandwidths	
Programming interfaces	<ul style="list-style-type: none"> ● Scriptable CLI ● DCNM web services API ● NX-API RESTful interfaces ● Onboard Python interpreter ● Embedded Event Manager (EEM) ● NX-OS Software scheduler 	
Industry Standard Compliance	<ul style="list-style-type: none"> ● Safety compliance ● CE Marking ● UL 60950 ● CAN/CSA-C22.2 No. 60950 ● EN 60950 ● IEC 60950 ● TS 001 ● AS/NZS 3260 ● IEC60825 ● EN60825 ● 21 CFR 1040 ● EMC compliance ● FCC Part 15 (CFR 47) Class A ● ICES-003 Class A ● EN 55022 Class A ● CISPR 22 Class A ● AS/NZS 3548 Class A ● VCCI Class A ● EN 55024 ● EN 50082-1 ● EN 61000-6-1 ● EN 61000-3-2 ● EN 61000-3-3 	
Power & Cooling	The Switch shall provide Redundant and hot swappable power supplies and should be platinum certified.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

10. Spine Switch

RESTRICTED

Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in CDC, NHQDC and DRDC to communicate with the Leaf switch for the SDN network.	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Manufacturing Country	To be mentioned by the bidder	
Spine Switch Architecture	<p>Switch must have at least</p> <ul style="list-style-type: none"> • 28 x 100/40-Gbps QSFP28 ports and • 8 x 400/100-Gbps QSFP-DD ports , <p>Bidder has to provide</p> <ul style="list-style-type: none"> • 20 x 40GE short range optical transceiver & • 08 x 100GE short range optical transceiver <p>with each devices from Day 1. All the modules are OEM original and same as "Switch" brand</p> <p>The switch must be spine-leaf based Software Data Centre architecture supported from day 1.</p> <p>The Spine switch must have minimum of 11.5 Tbps throughput or more.</p> <p>All relevant software, licenses and hardware for mentioned features should be quoted along with switch from Day-1.</p> <p>The proposed switches must be using the latest chipsets developed by the respective switch OEM.</p> <p>All the Spine switches will be connected to Leaf switches with 100GE connectivity from day 1 and it can be upgraded to 100/400GE in future with optical module up gradation.</p> <p>Switch should support port-side intake air-flow exhaust</p> <p>Switch should be provided with 19" Rack mountable with necessary mounting kit</p> <p>Switch should have N+1 redundant, hot-swappable fan modules and power supplies with power cords provided as per site requirement</p> <p>Switch should support both AC and DC power supply options. Bidders must propose with dual AC power supply.</p> <p>Switch should have Gigabit RJ45 & 1G SFP Port for OOB Management in separate VRF</p>	
	Switch throughput must be minimum of 11.5 Tbps or more	

RESTRICTED

Scalability & Performance Requirement	Switch should support packet throughput of min. 4.0 bpps or more	
	Switch should support at least 80MB buffer or more.	
	Switch should support minimum 32GB Memory , 128GB SSD drive.	
	Switch hardware should be capable of supporting:	
	1. 32K multicast routes	
	2. 895 K ipv4 route prefixes	
	3. 895 K host routes	
	4. 255K Overlay MAC addresses	
	5. 16000 VRF's	
Features Requirement	6. Cluster should have support more the 1200 edge port.	
	7. Number of (NAT) entries: Minimum 1000	
	Switch should automate the provisioning process of configuration of switches that are being deployed in the network for Day 1 deployment.	
	Should support Standard & Extended ACLs using L2, L3 and L4 fields	
	Switch should have configurable Unified forwarding table.	
	should support Rapid-Per Vlan Spanning Tree protocol, MST, Root Guard, and Bridge Assurance	
	Should support Private VLAN or Equivalent feature.	
	should support LACP: IEEE 802.3ad	
	Should Support line rate ingress and egress ACL filtering: Allow and deny, port filters, VLAN filters, and routed filters, including filters on management port	
	Should support VRRPv3	
	Should support Dynamic Arp Inspection, DHCP Snooping, IP Source Guard, IPv6 Security features like RA Guard and DHCPv6 Snooping	
	Switch should be able to provide security from layer 2 broadcast, multicast and unknown unicast by rate limiting such traffic.	
	Should have support for QoS policies including shaping, weighted random early detection, and explicit congestion notification features.	
	Should support Modular QoS CLI or equivalent mechanism wherein traffic can be segregated into categories and policies created per category, which can be applied to ingress/egress interfaces.	
	Should support both static and dynamic NAT	
	Should support multicast to act as leaf in fabric with flood and learn behavior.	
	Should support BFD	
Should support at least 256 VxLAN tunnel endpoint 's in the fabric.		
Switch must support VxLAN Switching/Bridging and VXLAN Routing without any performance degradation		
Should support VxLAN Routing from Day 1		

RESTRICTED

	Should support VRF Aware VXLAN Routing from Day 1	
	Should support VxLAN Network with MP-BGP EVPN Control Plane from Day 1	
	Should support VPC/Multi-chassis LAG with active-active forwarding with VxLAN for scalability and better traffic handling in data center.	
	Should support Standard & Extended ACLs using L2, L3 and L4 fields	
Monitoring and Management	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
	Should support SNMP v2 and v3	
	Should have Control plane Packet Capture functionality for troubleshooting purpose	
	Should support syslog	
	SSH v2 for CLI access with Secure interface login and password	
	Should support configurable telemetry for various device and protocol parameters.	
	Should support Net flow version 9 or sFlow v5	
	Should support Encapsulated Remote SPAN with selective traffic mirroring using ACL or filters	
	Should be able to export real-time flow table entries to monitoring/analytics software.	
	Should support secure guest shell access for installing 3rd party apps on the switch.	
	Should support streaming telemetry of control plane, flow table and environmental variables	
Gartner or Forrester Report	OEM/Solution must be in the Gartner's or Forrester Leader's Quadrant report for Data Centre SDN as per the 2022/2023-year report.	
Common Criteria Certification	The solution must be Common Criteria certified.	
ISO 9001 / 14001 Certification	The OEM/Manufacturer should have ISO 9001 or ISO 14001 certification.	
Design and Implementation Scope	Respective bidder also needs to ensure that the final deployment of the data center solution is done based on the standards design guideline and best practices keeping in mind the DC compliance requirements and operational requirements.	
	The validated design should take into consideration for scalability, modularity, and resiliency aspects of the data center as well as optimization from space, power and cooling perspective.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

RESTRICTED

Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	
--------------------------------	--	--

12. Border Leaf Switch		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in CDC, NHQDC and DRDC to communicate with the Spin switch for the SDN network. The Firewall, Load Balancer, WAF and all other core security devices will be connected in this switch.	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed OEM should be listed in Gartner Leader Quadrant for Data Centre Networking for last 2 years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
	All relevant software, licenses and hardware for mentioned features should be quoted along with switch from Day-1.	
	The proposed switches must be using the latest chipsets developed by the respective switch OEM.	
	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
	Switch should support the complete STACK of IPv4 and IPv6 services. Switch must have IPv6 phase 2 ready logo certifications.	
	The Switch used have the capability to function in line rate for all ports	
Hardware and Interface Requirement	Switch should have the following interfaces:	
	<ul style="list-style-type: none"> • Minimum 48 ports support 1/10/25 Gbps SFP ports for host connectivity and • 6 x 40/100Gbps QSFP28 ports for Fabric connectivity. Bidder has to provide <ul style="list-style-type: none"> • 20 x 10/25GE short range optical transceiver + • 06 x 10GE Copper transceiver + 	

RESTRICTED

	<ul style="list-style-type: none"> • 05 x 10G DAC 10 Meter & • 05 x 25G DAC 5 Meter + • 04 x 40GE optical transceiver with each devices from Day 1. <p>All the modules are OEM original and same as "Switch" brand</p>	
	Switch should have console port for local management & management interface for Out of band management	
	Must have 1 RU fixed form factor	
Performance Requirement	Modular OS with dedicated process for each routing protocol	
	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high availability during primary controller failure	
	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	
	Switch Should have Minimum 6 Core Processor, System memory Minimum 32GB and Storage Minimum 126 GB SSD from Day One.	
	Switch should support minimum 1000 VRF instances with route leaking functionality	
	The switch should support Minimum 896,000LPM routes	
	The Switch should support intelligent buffer management with a minimum buffer of 40MB.	
	The switch should have Maximum number of MAC address 512,000k.	
	The switch should support Minimum 127K multicast routes	
	Switch should support Minimum 4000 VLANs	
	Switch should support 64 nos of ECMP paths	
	Switch should support minimum 3.25Tbps of switching Bandwidth and minimum 1.1Billion packets per second (bps).	
Network Virtualization Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)	
	Switch should support VXLAN (RFC7348) and EVPN symmetric IRB (RFC 7432) for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data centre	
Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
	Switch should support VLAN Trunking (802.1q)	
	Switch should support VLAN tagging (IEEE 802.1q)	
	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	

RESTRICTED

		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
		Switch should support layer 2 extension over VXLAN (RFC7348) across all Datacentre to enable VM mobility & availability	
		<u>Switch should support FCoE from day 1.</u>	
		The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
		Maximum number of port channels should be 500	
		Maximum no of ports in the port channel link should be 32	
		The switch should support BGP EVPN (RFC 7432) Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
Layer3 Features		Switch should support static and dynamic routing	
		Switch should support segment routing and VRF route leaking functionality from day 1	
		Switch should support Segment Routing and Layer3 VPN over Segment Routing	
		Switch should support multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
		Switch should provide multicast traffic reachable using:	
		a. PIM-SM (RFC 4601)	
		b. PIM-SSM (RFC 3569)	
		Support Multicast Source Discovery Protocol (MSDP) (RFC 3618)	
		Switch Should Support IGMP v1, v2 and v3	
Quality Service	of	Switch system should support 802.1P classification and marking of packet using:	
		a. CoS (Class of Service)	
		b. DSCP (Differentiated Services Code Point)	
		Switch should support for different type of QoS features for real time traffic differential treatment using	
		a. Weighted Random Early Detection	
		b. Strict Priority Queuing	
		Switch should support Rate Limiting - Policing and/or Shaping	
		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
Security		Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
		Switch should support for external database for AAA using:	
		a. TACACS+	

RESTRICTED

	b. RADIUS	
	Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
	Switch platform should support MAC Sec (802.1AE) encryption in hardware all ports including uplink & downlink.	
	VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware	
	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
	Switch should support DHCP Snooping	
	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
	Switch should support IP Source Guard to prevents a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. IEEE 802.1ae MAC Security (MACsec) support on all ports with speed greater than or equal to 10-Gbps, allows traffic encryption at the physical layer and provides secure server, border leaf, and leaf-to-spine connectivity from day 1.	
	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
	The Switch should support LLDP.	
	Switch should support Spanning tree BPDU protection	
Manageability	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
	Switch should provide remote login for administration using:	
	a. Telnet	
	b. SSHv2	
	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
	The switch must have at least 288,000 hours Mean Time Between Failure (MTBF) for hardware reliability.	

RESTRICTED

	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
	a. SNMP v1 and v2, SNMP v3 with Encryption	
	Switch should provide different privilege for login in to the system for monitoring and management	
	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
	• Flow path trace (ingress to egress switch)	
	• Per Flow Hop by Hop packet drop with reason of drop	
	• Per Flow latency (per switch and end to end)	
Availability	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
	Switch should provide gateway level of redundancy Ip V.4 and IP V.6 using HSRP/VRRP	
	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
Miscellaneous points	Power cable (As per C13-C14 Connectors, 2 Meter Length) as per customer requirement to be provided. All Cables shall be factory-terminated.	
	All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
	All the components should be from same OEM.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

13. Leaf Switch		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in CDC, NHQDC and DRDC to communicate with the Spin switch for the SDN network. All the Servers in the Core will be connected in this switch.	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	

RESTRICTED

Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed OEM should be listed in Gartner Leader Quadrant for Data Centre Networking for last 2 years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
	All relevant software, licenses and hardware for mentioned features should be quoted along with switch from Day-1.	
	The proposed switches must be using the latest chipsets developed by the respective switch OEM.	
	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
	Switch should support the complete STACK of IPv4 and IPv6 services. Switch must have IPv6 phase 2 ready logo certifications.	
	The Switch used have the capability to function in line rate for all ports	
Hardware and Interface Requirement	Switch should have the following interfaces: <ul style="list-style-type: none"> • Minimum 48 ports support 1/10/25 Gbps SFP ports for host connectivity and • 6 x 40/100Gbps QSFP28 ports for Fabric connectivity. Bidder has to provide <ul style="list-style-type: none"> • 20 x 10/25GE short range optical transceiver + • 6 x 10GE Copper transceiver + • 10 x 1GE short range optical transceiver • 05 x 10G DAC 5 Meter & • 05 x 25G DAC 10 Meter + • 4 x 40GE optical transceiver with each devices from Day 1. All the modules are OEM original and same as "Switch" brand 	
	Switch should have console port for local management & management interface for Out of band management	
	Must have 1 RU fixed form factor	
Performance Requirement	Modular OS with dedicated process for each routing protocol	
	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high availability during primary controller failure	
	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	

RESTRICTED

	Switch Should have Minimum 6 Core Processor, System memory Minimum 32GB and Storage Minimum 126 GB SSD from Day One.	
	Switch should support minimum 1000 VRF instances with route leaking functionality	
	The switch should support Minimum 896,000LPM routes	
	The Switch should support intelligent buffer management with a minimum buffer of 40MB.	
	The switch should have Maximum number of MAC address 512,000k.	
	The switch should support Minimum 127K multicast routes	
	Switch should support Minimum 4000 VLANs	
	Switch should support 64 nos of ECMP paths	
	Switch should support minimum 3.25Tbps of switching Bandwidth and minimum 1.1Billion packets per second (bps).	
Network Virtualization Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)	
	Switch should support VXLAN (RFC7348) and EVPN symmetric IRB (RFC 7432) for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data centre	
Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
	Switch should support VLAN Trunking (802.1q)	
	Switch should support VLAN tagging (IEEE 802.1q)	
	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
	Switch should support layer 2 extension over VXLAN (RFC7348) across all Datacentre to enable VM mobility & availability	
	<u>Switch should support FCoE from day 1.</u>	
	The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
	Maximum number of port channels should be 500	
	Maximum no of ports in the port channel link should be 32	
	The switch should support BGP EVPN (RFC 7432) Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
Layer3 Features	Switch should support static and dynamic routing	
	Switch should support segment routing and VRF route leaking functionality from day 1	

RESTRICTED

		Switch should support Segment Routing and Layer3 VPN over Segment Routing	
		Switch should support multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
		Switch should provide multicast traffic reachable using:	
		a. PIM-SM (RFC 4601)	
		b. PIM-SSM (RFC 3569)	
		Support Multicast Source Discovery Protocol (MSDP) (RFC 3618)	
		Switch Should Support IGMP v1, v2 and v3	
Quality Service	of	Switch system should support 802.1P classification and marking of packet using:	
		a. CoS (Class of Service)	
		b. DSCP (Differentiated Services Code Point)	
		Switch should support for different type of QoS features for real time traffic differential treatment using	
		a. Weighted Random Early Detection	
		b. Strict Priority Queuing	
		Switch should support Rate Limiting - Policing and/or Shaping	
		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
Security		Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
		Switch should support for external database for AAA using:	
		a. TACACS+	
		b. RADIUS	
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
		Switch platform should support MAC Sec (802.1AE) encryption in hardware all ports including uplink & downlink.	
		VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware	
		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
		Switch should support DHCP Snooping	
		Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	

RESTRICTED

	Switch should support IP Source Guard to prevents a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. IEEE 802.1ae MAC Security (MACsec) support on all ports with speed greater than or equal to 10-Gbps, allows traffic encryption at the physical layer and provides secure server, border leaf, and leaf-to-spine connectivity from day 1.	
	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
	The Switch should support LLDP.	
	Switch should support Spanning tree BPDU protection	
Manageability	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
	Switch should provide remote login for administration using:	
	a. Telnet	
	b. SSHv2	
	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
	The switch must have at least 288,000 hours Mean Time Between Failure (MTBF) for hardware reliability.	
	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
	a. SNMP v1 and v2, SNMP v3 with Encryption	
	Switch should provide different privilege for login in to the system for monitoring and management	
	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
	• Flow path trace (ingress to egress switch)	
	• Per Flow Hop by Hop packet drop with reason of drop	
	• Per Flow latency (per switch and end to end)	

RESTRICTED

Availability	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
	Switch should provide gateway level of redundancy Ip V.4 and IP V.6 using HSRP/VRRP	
	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
Miscellaneous points	Power cable (As per C13-C14 Connectors, 2 Meter Length) as per customer requirement to be provided. All Cables shall be factory-terminated.	
	All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
	All the components should be from same OEM.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

14. POE LAN Switch		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used across the BNNET for the access layer to connect all the end points.	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Environmental	Maintain International Quality Environmental Safety standard	
Form factor	Rack Mountable with Rack Mounting Kit	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Architecture	The Switch should have <ul style="list-style-type: none"> • 24 x 10/100/1000 Base-T POE+ (370W) from day 1 & • 740w scalable with secondary power supply and • 4 x 1G/10G SFP slots. 	

RESTRICTED

	<p>The bidder must include</p> <ul style="list-style-type: none"> • 2 x 10G base LR optical transceiver with each switches from day 1. <p>All the modules are OEM original and same as "Switch" brand</p>	
	The switch should support at least 125 Gbps switching capacity and 92 Mpps forwarding rate	
	Switch should have 2GB RAM and 4 GB Flash.	
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.	
	Switch should have slot/ports (excluding uplinks ports) for minimum 80 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack	
	Switch must comes with hardware stacking capabilities from Day 1	
	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.	
	Switch should be able to support 3000 IPV4 & 1500 IPV6 routing entries from Day 1	
	Switch should support minimum 500 Switched Virtual Interfaces.	
	The switch should support Jumbo frames of 9198 bytes	
	The Switch must have dual redundant power supply from Day 1	
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture	
	The Switch should support Layer 2 features, Routed Access (RIP, OSPF), Policy Based Routing, PIM Stub Multicast, Private VLAN, VRRP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder from Day 1	
	The Switch should support IS-IS, BSR, MSDP, IP SLA, OSPF, VRF, VXLAN, LISP	
	The proposed switch should be software defined networking capable and be able to at least integrate easily with the SDN controller from the same OEM.	
	Switch shall support application visibility and traffic monitoring with minimum 16K netFlow/sflow/jflow entries.	
	Switched should support both front and back beacon LEDs for easy identification of the switch being accessed.	
	Switches should have hardware support to connect a Bluetooth dongle to your switch, enabling you to use this wireless interface as an IP management port interface.	
High availability & Resiliency	Switch should support redundant field replaceable power supplies	
	Switch should support redundant field replaceable fans	
	Switch should support cross-stack EtherChannel.	

RESTRICTED

L2 Features	The switch should support Automatic Negotiation of Trucking Protocol, to help minimize the configuration & errors	
	The switch should support IEEE 802.1Q VLAN encapsulation	
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence	
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability	
	The switch should support Spanning-tree root guard to prevent other edge switches becoming the root bridge.	
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN	
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth	
	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.	
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.	
	The switch should support IGMP v1, v2 Snooping	
	Switch should support IPv4 and IPv6The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.	
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA	
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions	
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration	
	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network	
	The switch should support MACSec-128 bit from Day 1	
Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring	

RESTRICTED

	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility	
	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG	
QoS	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

15. Industrial Grade Ethernet switch		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in all the Jetty to connect with the ships secured in the Jetty.	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Environmental	Maintain International Quality Environmental Safety standard	
Form factor	Rack Mountable with Rack Mounting Kit	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Architecture	<p>The Switch should have</p> <ul style="list-style-type: none"> • 8 x 1G Base-T POE+ (240W) & 360 w scalable with extra module for future scalability and • 2 x 1G SFP uplink port. <p>The bidder must include</p> <ul style="list-style-type: none"> • 2 x 1G Single Mode Rugged optical transceiver with each switches from day 1. 	

RESTRICTED

	All the modules are OEM original and same as "Switch" brand	
	The switch should support at least 125 Gbps switching capacity and 92 Mpps forwarding rate	
	Switch should have 4GB RAM and 1.5 GB Flash.	
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.	
	Switch should be able to support 3000 IPV4 & 512 IPV6 routing entries from Day 1	
	Switch should support minimum 256 VLAN	
	The switch should support Jumbo frames of 8996 bytes	
	The Switch must have AC & DC power supply option . Should have redundant power supply options.	
	The Switch should support Layer 2 features, IEEE 802.1, 802.3 standard, NTP, UDLD, LLDP, unicast MAC filter, PAgP, LACP VTPv2, VTPv3, EtherChannel, Q-in-Q tunneling, voice VLAN, PVST+, MSTP, and RSTP	
	The Switch should support CIP Ethernet/IP, IEEE 1588 PTP v2 (default and power)1, PROFINET	
	IEC 62443-4-1	
	IEC 62443-4-2	
	EN 61000-6-2 Industrial Immunity	
	EN 61000-6-4 Industrial Emissions	
	EN 61000-6-1 Light Industrial Immunity	
	EN 61326-1 Measurement, Control and Laboratory Equipment	
	EN 61131-2 (EMC - Emission and Immunity)	
	IEEE 1613 Electric Power Stations Communications Networking	
	EN/IEC 61850-3 Electric Substations Communications Networking	
	ODVA Industrial EtherNet/IP	
	NEMA TS 2-2016	
	AREMA C and S section 11, 19	
	IP30	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

16. DC-DR Replicator Switch (IPN)		
Feature List	Feature Description	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed OEM should be listed in Gartner Leader Quadrant for DC Networking for last 2 years	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	
Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
	All relevant software, licenses and hardware for mentioned features should be quoted along with switch from Day-1.	
	The proposed switches must be using the latest chipsets developed by the respective switch OEM.	
	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy	
	Switch should support the complete STACK of IPv4 and IPv6 services. Switch must have IPv6 phase 2 ready logo certifications.	
	The Switch used have the capability to function in line rate for all ports	
Hardware and Interface Requirement	Switch should have the following interfaces: <ul style="list-style-type: none"> • Minimum 24 ports support 1/10/25 Gbps SFP ports for host connectivity and • 6 x 40/100Gbps QSFP28 ports for Fabric connectivity. Bidder has to provide <ul style="list-style-type: none"> • 10 x 10GE short range optical transceiver + • 4 x 1GE Copper transceiver + • 4 x 40GE short range optical transceiver + • 2 x 40GE Long range (Min. 9.5KM operating ranges) optical transceiver with each devices from day 1. The modules are OEM original and same as "Switch" brand	
	Switch should have console port for local management & management interface for Out of band management	
	1 RU fixed form factor	
Performance Requirement	Modular OS with dedicated process for each routing protocol	

RESTRICTED

	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high availability during primary controller failure	
	Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e., graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	
	Switch Should have Minimum 6 Core Processor, System memory Minimum 30 GB and Storage Minimum 120 GB SSD from Day One.	
	Switch should support minimum 1000 VRF instances with route leaking functionality	
	The switch should support Minimum 1,750,000 LPM routes	
	The Switch should support intelligent buffer management with a minimum buffer of 40MB.	
	The switch should have Maximum number of MAC address 512k.	
	The switch should support Minimum 125K multicast routes	
	Switch should support Minimum 4000 VLANs	
	Switch should support 64 nos of ECMP paths	
	Switch should support minimum 3.5 Tbps of switching Bandwidth and minimum 1.15 billion packets per second (bps).	
Network Virtualization Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)	
	Switch should support VXLAN (RFC7348) and EVPN symmetric IRB (RFC 7432) for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center	
Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
	Switch should support VLAN Trunking (802.1q)	
	Switch should support VLAN tagging (IEEE 802.1q)	
	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
	Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
	Switch should support layer 2 extension over VXLAN (RFC7348) across all Datacenter to enable VM mobility & availability	
	The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
	Maximum number of port channels should be 500	
	Maximum no of ports in the port channel should be 32	

RESTRICTED

		The switch should support BGP EVPN (RFC 7432) Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
Layer3 Features		Switch should support static and dynamic routing	
		Switch should support segment routing and VRF route leaking functionality from day 1	
		Switch should support Segment Routing and Layer3 VPN over Segment Routing	
		Switch should support multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
		Switch should provide multicast traffic reachable using:	
		a) PIM-SM (RFC 4601)	
		b) PIM-SSM (RFC 3569)	
		Support Multicast Source Discovery Protocol (MSDP) (RFC 3618)	
	Switch Should Support IGMP v1, v2 and v3		
Quality Service of		Switch system should support 802.1P classification and marking of packet using:	
		a) CoS (Class of Service)	
		b) DSCP (Differentiated Services Code Point)	
		Switch should support for different type of QoS features for real time traffic differential treatment using:	
		a) Weighted Random Early Detection	
		b) Strict Priority Queuing	
		Switch should support Rate Limiting - Policing and/or Shaping	
	Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
Security		Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
		Switch should support for external database for AAA using:	
		a) TACACS+	
		b) RADIUS	
		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
		Switch platform should support MAC Sec (802.1AE) encryption in hardware	
		VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware	
		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
	Switch should support DHCP Snooping		

RESTRICTED

	Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
	Switch should support IP Source Guard to prevents a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. IEEE 802.1ae MAC Security (MACsec) support on all ports with speed greater than or equal to 10-Gbps, allows traffic encryption at the physical layer and provides secure server, border leaf, and leaf-to-spine connectivity from day 1.	
	Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port	
	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
	The Switch should support LLDP.	
	Switch should support Spanning tree BPDU protection	
Manageability	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
	Switch should provide remote login for administration using:	
	a) Telnet	
	b. SSHv2	
	Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
	The switch must have at least 286,000 hours Mean Time Between Failure (MTBF) for hardware reliability.	
	Switch should support for management and monitoring status using different type of Industry standard NMS using:	
	SNMP v1 and v2, SNMP v3 with Encryption	
Switch should provide different privilege for login in to the system for monitoring and management	Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
	The Switch Should support monitor events and take corrective action like a script when the monitored events occur.	
	• Flow path trace (ingress to egress switch)	
	• Per Flow Hop by Hop packet drop with reason of drop	
	• Per Flow latency (per switch and end to end)	

RESTRICTED

Availability	Switch should have provisioning for connecting to 1:1/N+1 power supply for usage and redundancy	
	Switch should provide gateway level of redundancy Ip V.4 and IP V.6 using HSRP/VRRP	
	Switch should support for BFD For Fast Failure Detection as per RFC 5880	
Miscellaneous Points	Power cable (As per C13-C14 Connectors, 2 Meter Length) as per customer requirement to be provided. All Cables shall be factory-terminated	
	All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software	
	All the components should be from same OEM	
Compliance & Reference	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available and accessible document	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

17. Out of Band Management Switch		
Feature List	Feature Description	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ-2019/2020	
Environmental	Maintain International Quality Environmental Safety standard	
Form factor	Rack Mountable with Rack Mounting Kit	
Part No	Bidder should submit BOQ of proposed device including the details' part numbers. Bidder should submit the required performance document for the proposed device.	

RESTRICTED

Architecture	<p>The Switch should have</p> <ul style="list-style-type: none"> • 48 x 10/100/1000 Base-T ports and • 4 x 1G/10G SFP slots. <p>The bidder must include</p> <ul style="list-style-type: none"> • 4 x 10G Short range optical transceiver with each switches from day 1. <p>All the modules are OEM original and same as "Switch" brand</p>	
	The switch should support at least 170 Gbps switching capacity and 125 Mpps forwarding rate	
	Switch should have 2GB RAM and 4 GB Flash.	
	The switch should support 16K MAC Addresses and 4000 VLAN IDs.	
	Switch should have slot/ports (excluding uplinks ports) for minimum 80 Gbps of stacking bandwidth with dedicated stacking ports and cables with minimum 8 switch in stack	
	Switch must comes with hardware stacking capabilities from Day 1	
	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.	
	Switch should be able to support 3000 IPV4 & 1500 IPV6 routing entries from Day 1	
	Switch should support minimum 500 Switched Virtual Interfaces.	
	The switch should support Jumbo frames of 9198 bytes	
	The Switch must have dual redundant power supply from Day 1	
General Features	Proposed switch should be enterprise grade switch with x86 based CPU architecture	
	The Switch should support Layer 2 features, Routed Access (RIP, OSPF), Policy Based Routing, PIM Stub Multicast, Private VLAN, VRRP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder from Day 1	
	The Switch should support IS-IS, BSR, MSDP, IP SLA, OSPF, VRF, VXLAN, LISP	
	The proposed switch should be software defined networking capable and be able to at least integrate easily with the SDN controller from the same OEM.	
	Switch shall support application visibility and traffic monitoring with minimum 16K netFlow/sflow/jflow entries.	
	Switched should support both front and back beacon LEDs for easy identification of the switch being accessed.	
	Switches should have hardware support to connect a Bluetooth dongle to your switch, enabling you to use this wireless interface as an IP management port interface.	

RESTRICTED

High availability & Resiliency	Switch should support redundant field replaceable power supplies	
	Switch should support redundant field replaceable fans	
	Switch should support cross-stack EtherChannel.	
L2 Features	The switch should support Automatic Negotiation of Trucking Protocol, to help minimize the configuration & errors	
	The switch should support IEEE 802.1Q VLAN encapsulation	
	The switch should support Spanning-tree PortFast and PortFast guard for fast convergence	
	The switch should support UplinkFast & BackboneFast technologies to help ensure quick failover recovery, enhancing overall network stability and reliability	
	The switch should support Spanning-tree root guard to prevent other edge switches becoming the root bridge.	
	The switch should support Voice VLAN to simplify IP telephony installations by keeping voice traffic on a separate VLAN	
	The switch should support Auto-negotiation on all ports to automatically selects half- or full-duplex transmission mode to optimize bandwidth	
	The switch should support Automatic media-dependent interface crossover (MDIX) to automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.	
	The switch should support Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD to allow for unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.	
	The switch should support IGMP v1, v2 Snooping	
	Switch should support IPv4 and IPv6The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighboring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.	
Network security features	The switch should support IEEE 802.1x providing user authentication, authorization and CoA	
	The switch should support SSHv2 and SNMPv3 to provide network security by encrypting administrator traffic during Telnet and SNMP sessions	
	The switch should support TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration	
	The switch should support MAC address notification to allow administrators to be notified of users added to or removed from the network	
	The switch should support MACSec-128 bit from Day 1	

RESTRICTED

Management features	Support SNMP, syslog, NetFlow or SFlow, Data telemetry collection and correlation for performance monitoring	
	Support sampled NetFlow/SFlow, Switched Port Analyzer, Remote SPAN, shared NetFlow/SFlow policy, RSPAN and packet capture tool like Wireshark for troubleshooting and network visibility	
	Support Network automation with Open PnP, Containers, Python scripting, NETCONF, RESTCONF using YANG	
QoS	Switch should support 802.1p Class of Service (CoS) and Differentiated Services Code Point (DSCP) field classification, Shaped Round Robin (SRR) scheduling, Committed Information Rate (CIR), and eight egress queues per port	
Compliance & Reference	Bidder must provide the detail compliance report with reference. The reference URL / information of RFP technical specification compliance should be publicly available and accessible document	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

18. SDN Controller		
Feature List	Feature Description	Bidder Response
Purpose	This device shall be used in CDC, NHQDC and DRDC to build the SDN network.	
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
General Requirement	Feature Set	
Fabric Definition	Proposed fabric must be the Clos network topology architecture defined using Spine, Leaf switches with VXLAN (RFC7348) overlay	
	Fabric should have achieve following functionalities:	
	Flexibility : Should allow workload mobility anywhere in the DC, across the Data Centre sites	

RESTRICTED

	Resiliency : The proposed fabric should be able to sustain multiple link and device (Leaf & Spine) failures with sub-second recovery	
	Performance: The proposed fabric should be able with use full cross sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi pathing. The proposed solution should have 3 node appliance which will be ensure N+1 design. Each Appliance should have min .Intel 16core processor,192GB Memory , 2.4TB SAS HDD from day1 . Solution should have capable to connect more then 1200 edge port from day1.	
	Deterministic Latency : The proposed fabric must provide predictable latency between any two endpoints connected to the fabric.	
	Multi-Data Centre design:- The proposed architecture should be extensive to multiple data centres and should have single management controller to push consistent policies across all the sites	
	Hardware and Interface Requirement	
	Fabric Connectivity should have the following properties:	
	Leaf switches to Spine connectivity should use uplink port using line rate 40/100G only	
	Each Leaf switch should connect each Spine switch using equal bandwidth uplink ports	
	All switches including Spine and leafs should be of line rate including access and uplink ports non-blocking. Datacentre Network & Enterprise Network, SDN Controller provider should be same OEM.	
Fabric Features	Fabric must support various Hypervisor encapsulation including VXLAN and 802.1q natively without any additional hardware/software or design change.	
	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.	
	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.	
	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.	
	Fabric must integrate with different virtual machine manager viz. VMware vCenter, Microsoft Hyper-V with System Center and manage virtualize networking from the single pane of Glass - Fabric Controller/SDN Controller	
	Fabric must support provide default gateway redundancy	
	Fabric must integrate with best of breed L4 - L7 Physical and virtual appliances and manage using single pane of glass - Fabric Controller / SDN Controller	

RESTRICTED

	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between any two endpoints on the fabric	
	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc	
Fabric Security Features	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service	
	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD	
	Fabric must support VM attribute based zoning and policy	
	Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment	
	Fabric must support true multi - tenancy	
	Fabric must act as a State-less distributed firewall with the logging capability	
	Fabric must be capable to provide services of L 4 - L7 services using physical or virtual appliances i.e. Firewall, ADC, IPS etc.	
Fabric management	Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of glass for managing, monitoring and provisioning the entire Fabric within Data Center & across all Data Centers'	
	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralised Management appliance or SDN Controller.	
	Centralised management appliance or SDN Controller must manages and provision rules on L4 - L7 Services physical and virtual appliance as well as integrate with Virtual Machine manager.	
	Centralised management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.	
	Centralised management appliance or SDN Controller must provide necessary report for compliance and audit.	
	Centralised management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX / OPENFLOW / OVSDB etc. or using Device APIs.	
	Centralised management appliance or SDN Controller must run in "N + 1" redundancy to provide availability as well as function during the split brain scenario	
	In Event of all Centralised management appliances or SDN Controllers fails, the fabric must function without	

	any performance degradation and with the current configuration.	
	Centralised management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.	
	All infrastructure required by fabric controllers to support the listed features and scale, should be provided by the bidder	
The SDN solution should have	Seamless integration of underlay and overlay networks end-to-end.	
	Common platform for managing physical and virtual environments	
	A centralized single point of management and visibility with full automation and zero touch provisioning, along with a real-time network health monitoring	
	Have a true built-in integration capabilities with hypervisors, to manage them and virtual switches without prior knowledge in Open stack.	
	Provide Centralized Service insertion with physical and virtual appliances and Integration with bare metal workloads, VMW ESXi, MSFT HyperV, OpenStack, Red Hat RHEV, Containers (Kubernetes, OpenShift, Cloud Foundry).	
	Work cohesively with all types of workloads including virtual machines, physical bare-metal servers, and containers	
	Provide Centralized True micro segmentation for physical and virtual workloads, without the need of external devices or software, using a white list model.	
	Automation of the configuration and management of intersite network interconnects across an IP backbone for both SDN Controller and Multi site Orcastation	
	Consistent multitenant policy across multiple sites, which allows IP mobility, disaster recovery, and active/active use cases for data centers	
	Capability to map tenants, applications, and associated networks to specific availability domains within the Multi-Site architecture for both SDN Controller and Multi site Orcastation	
	Hybrid cloud and multi-cloud orchestration supporting on-premises One prem sites and public cloud sites like (AWS and Azure)	
	Data center interconnectivity	
	Scale out sites and leaf switches based on resource growth	
Secure networking with a zero-trust security model and innovative micro-segmentation security feature		

RESTRICTED

	The architecture should allow interconnect separate cluster domains (fabrics) like DC & DR , each representing a different region, all part of the same Domain . It should ensure multitenant Layer 2 and Layer 3 network connectivity across sites, and it also extends the policy domain end-to-end across the entire system.	
Warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

19. Multi Site Orchestration System		
Item	Required Specification	Bidder Response
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
	It should help to Maintain business continuity by having backward compatibility with legacy protocols.	
	It should help to Detect changes in configuration or operational state before and after switch-upgrades and validate across multiple checks.	
	It should be a One-stop shop for information about assurance on policy and configuration analysis changes.	
	It should explore associations and connectivity across multiple sites and understand the state of network deployment using powerful natural-language querying	
	It should provide Comprehensive view of health drift between any two points in time, minimizing the change window	
	IT should also provide Comprehensive view of policy/config drift between two points in time, minimizing troubleshooting time	
	It should be able to Gather evidence from past data. Peek back in time to look at a specific sequence of events and gather intelligent insights.	
	It should use Flow Telemetry to minimize troubleshooting time through automated root-cause analysis of data plane anomalies, such as packet drops, latency, workload movements, routing issues, ACL drops, and more. Monitor flow rate usage to optimize performance.	
	It should Expose and locate invisible microbursts. Find out congestion hot spots and protect application performance.	
	It should Use detailed statistics and state information of PIM, IGMP, and IGMP-snooping protocols to monitor multicast control plane health	

RESTRICTED

	<p>It should Compare and contrast time-synced data of multiple parameters to derive deeper understanding of issues and behaviors. Know the impacted endpoints, applications, and flows due to network anomalies.</p>	
	<p>It should tag anomaly events to the right team member for faster resolution</p>	
	<p>It should Provide efficient capacity planning to maintain top network performance. Get fabric-wide visibility of resource utilization and historical trends. Detect components exceeding capacity thresholds ahead of time. Examples: TCAM, routes, ACL entries, ports, tenants, VRFs and many more.</p>	
	<p>It should proactively monitor and report environmental anomalies by leveraging telemetry data from hardware sensors such as CPU, memory, disk, power supply, fan speed, and temperature.</p>	
	<p>It should use detailed data-plane statistics to diagnose, locate, and remediate issues. Monitor and use protocol anomalies and state information to remediate BGP, vPC, LACP, CDP, and LLDP problems.</p>	
	<p>It should create custom dashboard views for your own preferred way of monitoring. Keep a close eye on parameters of your choice.</p>	
	<p>It should be able to Locate virtual machines, bare-metal hosts, and other endpoints in the data center fabric. Use historical data to track their movements.</p>	
	<p>It should be able to Use your natural visio-spatial ability to explore, navigate, discover, and zoom into issues. Visualize logical constructs such as tenant, VRF, VLAN, and more on top of the physical topology. Perform rapid troubleshooting using filters to focus on problematic nodes.</p>	
	<p>It should Stay up to date on new software and hardware availability. Be up to date on hardware and software end-of-sale announcements, and get lead time to plan for upgrades.</p>	
	<p>It should Get notified and take necessary action to stay secure and in compliance. Get instant visibility into any applicable bugs. Prevent unscheduled outages.</p>	
	<p>It should help Minimize risk of running End-of-Sale (EoS) or End-of-Life (EoL) devices. View current and project the future status of network software and hardware inventory against known EoS/EoL notices to ensure conformance.</p>	
	<p>IT should help to Automate the mundane, repetitive tasks of log collection, and attach them to TAC Service Requests (SRs). Delegate additional log collection to the TAC team.</p>	
	<p>It should be able to Verify software and hardware programming consistency across all available traffic paths between endpoints. Track per hop information and behavior.</p>	

RESTRICTED

It should be able to give offline alerts about network health using the email-notification facility.	
It must help to Validate Low-Level Design configurations across your environment for both online and offline sites.	
It must be able to Track the end-to-end flow across an externally connected device such as a firewall, to help locate data-plane issues across device silos and deduce the locations of packet drops.	
It should help to Export Anomaly and Advisory summaries through email and PDFs.	
It should have integrations with third-party IT applications.	
It must help to Gain cross-domain visibility into virtualized workload data, and perform rapid troubleshooting with qualitative and quantifiable data on Virtual Environment/VMWare.	
It Must help to Reduce MTTR with one-click automated fixes of known behaviors	
It must help with Configuration Compliance and ensure that naming and golden template configurations meet IT requirements for enhanced productivity while Communication Compliance ensures that regulatory and business communication always meets compliance	
Predict the impact of the intended configuration changes to drive insight-driven change management	
Manage TCAM capacity resources and security policy with advanced utilization analysis	
Ensure that intended configuration policies are deployed across multiple sites.	
Should have Open APIs to manage the switch through remote procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
Should support SNMP v2 and v3	
Should have Control plane Packet Capture functionality for troubleshooting purpose	
Should support syslog	
SSH v2 for CLI access with Secure interface login and password	
Should support configurable telemetry for various device and protocol parameters.	
Should support Net flow version 9 or sFlow v5	
Should support Encapsulated Remote SPAN with selective traffic mirroring using ACL or filters	
Should be able to export real-time flow table entries to monitoring/analytics software.	
Should support secure guest shell access for installing 3rd party apps on the switch.	
Should support streaming telemetry of control plane, flow table and environmental variables	

RESTRICTED

Hardware Specifications	Bidder should propose OEM Appliance/ Virtual Appliances for proposed solutions. For VM instances, Bidder need to mention and propose necessary Hardware details for catering the requirements.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

Technical Specification of Firewall

20. Core Firewall		
Feature List	Feature Description	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC for quality assurance	
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry recommendations	The Firewall solution must be rated leader in the Magic Quadrant Report for Enterprise Firewall published by Gartner or Forrester wave report.	
Hardware Architecture	The appliance based security platform should provide firewall, Application Visibility Control, IPS and Advance Malware Protection functionality in a single appliance from day one. Solution should have zero-day threat protection coverage from day one. Bidder has to provide NGIPS, AMP & Web Filtering license for 3 Years.	
	The appliance should support at least <ul style="list-style-type: none"> • 8 x 10G SFP+ and • 8 x 1/10/25G SFP+ ports from day one and should be scalable to provide additional <ul style="list-style-type: none"> • 2 x 100G or • 4 x 40/100/200 ports if required in future. Bidder has to provide <ul style="list-style-type: none"> • 8 x 10GE short range optical transceiver • 8 x 10/25 GE short range optical transceiver with each devices from Day 1. All the modules are OEM original and same as "Firewall" brand	
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 256 GB of RAM and 32 CPU Cores.	

RESTRICTED

	Proposed firewall should not consume more than 1RU of rack space	
Management ports	Two 1/10/25-Gbps SFP28 ports	
Performance & Scalability	Should support at least 60 Gbps of Firewall throughput.	
	There should not be degradation in performance on enabling application control (AVC) and Intrusion Prevention (IPS) security features, and should support at least 60Gbps of NGFW (FW, AVC and IPS).	
	Firewall should support at least 14.5 Million concurrent sessions with application visibility turned on	
	Firewall should support at least 20000 VPN peers	
	Firewall should support at least 3,49,000 new connections per second with application visibility turned on	
	Firewall should have integrated redundant hot-swappable fans	
NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc	
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	Should support Multicast protocols like IGMP, PIM, etc	
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness.	
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy		

RESTRICTED

	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Should be capable of detecting and blocking IPv6 attacks.	
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
	Firewall should support time based policies, where policies can be enforced for certain time ranges like hours, days, weeks, etc.	
	Firewall should provide integrated DNS security, where firewall should block traffic based on the domain name requested by a client	
	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
	The management platform must be a dedicated OEM appliance and VM running on server will not be accepted	
	The management appliance should have 2 x 10G port and integrated redundant power supply from day one	

RESTRICTED

	The management platform must be able to store record of 15000 user or more & at least 30 Million IPS events.	
	The management platform must provide a highly customizable dashboard.	
	The management platform must domain multi-domain management	
	The management platform must provide centralized logging and reporting functionality	
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
	Should support troubleshooting techniques like Packet tracer and capture	
	Should support REST API for monitoring and config programmability	
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
	The centralized management platform must not have any limit in terms of handling logs per day	
	Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one	
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	The management platform support running on-demand and scheduled reports	
	The management platform must risk reports like advanced malware, attacks and network	
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
URL Filtering Features	Should must support URL threat intelligence feeds to protect against threats	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 270 million of URLs in more than 78 categories.	
	Should support safe search for YouTube EDU enforcement	

RESTRICTED

Hardware	Temperature Operating: 0 to 40°C	
	Temperature Nonoperating: -20 to 65°C	
	Humidity: 10 to 85% noncondensing	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

21. WAN Firewall		
Item	Required Specification	Bidder Response
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Industry recommendations	The Firewall solution must be rated leader in the Magic Quadrant Report for Enterprise Firewall published by Gartner or Forrester wave report.	
Hardware Architecture	The appliance based security platform should provide firewall, Application Visibility Control, IPS, and Advance Malware Protection, Web Filtering functionality in a single appliance from day one. Solution should have zero-day threat protection coverage from day one.	
	The appliance should have at least <ul style="list-style-type: none"> • 8 x 10GE RJ45 & • 8 x 1/10GE SFP+ ports populated with • 8 no's of 10GE SR SFP module. All SFP should be from the same OEM.	
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128-GB of RAM and 16 CPU Cores.	
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.	
	Proposed firewall should not consume more than 1RU of rack space	
Performance & Scalability	Should support at least 20 Gbps of Firewall throughput with 1024B packet size.	
	There should not be degradation in performance on enabling application control (AVC) and Intrusion Prevention (IPS) security features, and should support at least 20 Gbps of NGFW (FW, AVC and IPS) with 1024B packet size.	
	Firewall should support at least 4,000,000 concurrent sessions with application visibility turned on	
	Firewall should support at least 7000 VPN peers. Bidder should propose 500 Client VPN license from Day one.	
	Firewall should support at least 1,60,000 new connections per second with application visibility turned on	

RESTRICTED

NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc	
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to- IPv6) functionality	
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	Should support Multicast protocols like IGMP, PIM, etc	
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness.	
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Should be capable of detecting and blocking IPv6 attacks.	
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		

RESTRICTED

	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
	Firewall should support time based policies, where policies can be enforced for certain time ranges like hours, days, weeks, etc.	
	Firewall should provide integrated DNS security, where firewall should block traffic based on the domain name requested by a client	
	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
Management	The solution should have separate hardware/ Virtual management appliance for centralized management of Firewalls and Logging & Reporting.	
	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
	The management platform can be a dedicated OEM appliance/ or Virtual appliances. For VM instances, Bidder need to mention and propose necessary Hardware details for catering the requirements.	
	The management platform must provide a highly customizable dashboard.	
	The management platform must domain multi-domain management	
	The management platform must provide centralized logging and reporting functionality	
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	

RESTRICTED

	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
	Should support troubleshooting techniques like Packet tracer and capture	
	Should support REST API for monitoring and config programmability	
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
	The solution should be able to give insights on hosts/users on the basis of Indicators of Compromise. Any license required for this should be included from day one.	
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	The management platform support running on-demand and scheduled reports	
	The management platform must risk reports like advanced malware, attacks and network	
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
URL Filtering Features	Should support URL threat intelligence feeds to protect against threats.	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 270 million of URLs in more than 78 categories.	
	Should support safe search for YouTube EDU enforcement	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

22. DMZ Firewall		
Item	Required Specification	Bidder Response
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Industry recommendations	The Firewall solution must be rated leader in the Magic Quadrant Report for Enterprise Firewall published by Gartner or Forrester wave report.	
Hardware Architecture	The appliance based security platform should provide firewall, Application Visibility Control, IPS, and Advance Malware Protection, Web Filtering functionality in a single appliance from day one. Solution should have zero-day threat protection coverage from day one.	
	The appliance should have at least <ul style="list-style-type: none"> • 8 x 10GE RJ45 & • 8 x 1/10GE SFP+ ports populated with • 8 no's of 10GE SR SFP module. All SFP should be from the same OEM.	
	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 128-GB of RAM and 16 CPU Cores.	
	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.	
	The proposed solution shouldn't use a proprietary ASIC hardware for any kind of performance Improvement. If option to disable ASIC is there than OEM must mention the performance numbers in datasheet.	
	Proposed firewall should not consume more than 1RU of rack space	
Performance & Scalability	Should support at least 20 Gbps of Firewall throughput with 1024B packet size.	
	There should not be degradation in performance on enabling application control (AVC) and Intrusion Prevention (IPS) security features, and should support at least 20 Gbps of NGFW (FW, AVC and IPS) with 1024B packet size.	
	Firewall should support at least 4,000,000 concurrent sessions with application visibility turned on	
	Firewall should support at least 7000 VPN peers. Bidder should propose 500 Client VPN license from Day one.	
	Firewall should support at least 1,60,000 new connections per second with application visibility turned on	

RESTRICTED

NG Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc	
	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat	
	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to- IPv6) functionality	
	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	Should support Multicast protocols like IGMP, PIM, etc	
	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness.	
	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Should support more than 25,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Should be capable of detecting and blocking IPv6 attacks.	
	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor		

RESTRICTED

	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.	
	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
	The detection engine should support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
	Firewall should support time based policies, where policies can be enforced for certain time ranges like hours, days, weeks, etc.	
	Firewall should provide integrated DNS security, where firewall should block traffic based on the domain name requested by a client	
	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
Management	The solution should have separate hardware/ Virtual management appliance for centralized management of Firewalls and Logging & Reporting.	
	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
	The management platform can be a dedicated OEM appliance/ or Virtual appliances. For VM instances, Bidder need to mention and propose necessary Hardware details for catering the requirements.	
	The management platform must provide a highly customizable dashboard.	
	The management platform must domain multi-domain management	
	The management platform must provide centralized logging and reporting functionality	
	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	

RESTRICTED

	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
	Should support troubleshooting techniques like Packet tracer and capture	
	Should support REST API for monitoring and config programmability	
	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
	The solution should be able to give insights on hosts/users on the basis of Indicators of Compromise. Any license required for this should be included from day one.	
	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
	The management platform support running on-demand and scheduled reports	
	The management platform must risk reports like advanced malware, attacks and network	
	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.	
URL Filtering Features	Should support URL threat intelligence feeds to protect against threats.	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 270 million of URLs in more than 78 categories.	
	Should support safe search for YouTube EDU enforcement	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

23. Core Firewall 2		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned by Bidder. (Preferably Checkpoint / Palo Alto).	
Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder.	
No of Core Firewall Units per Site	2 Units in HA	
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content / URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).	
3rd Party Test Certification	The offered hardware / model must maintain global standard certification for Safety, compliance and Environmental certificate. Vendor must mention certificate names.	
	The proposed OEM must be Leader in the latest Network Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof.	
	The protection rate of the proposed solution shall be 96% or above as per the latest published Enterprise Firewall Test Results from published by Cyber Rating. Reports to be submitted by the bidder as proof.	
General Security Features	The proposed solution shall provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic from day one	
	The proposed solution shall reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content from day one	
	The proposed solution shall prevent all known threats – Network DoS/DDoS, Malware, Spyware, Ransomware, Trojan, C&C, Malicious & Phishing Websites from day 1	
	The proposed solution shall Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior from day one	
	The proposed solution shall Inspect and control applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic from day one	

RESTRICTED

	All firewall must come with minimum 5 Virtual Contexts from day 1	
Storage	Proposed NGFW appliance must have 2 SSD and minimum 480 GB SSD of internal system storage.	
Memory (DRAM)	Minimum 128 GB RAM from day 1.	
Power	Full redundant Power Supplies from day 1.	
Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> 8x 1GE/10GE SFP and SFP+ ports/interfaces fully populated with short range 10G SFP+ transceivers of same OEM as NGFW from day 1 	
	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> 8x 10GE/25GE SFP+ and SFP28 compatible ports/interfaces fully populated with short range 25G Base transceiver of same OEM as NGFW from day 1. 	
	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> 2x 40G/100G ports/interfaces fully populated with short range 40G Base transceiver of same OEM as NGFW from day 1. 	
	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> 2x 10G/25G purposeful dedicated HA ports/interfaces fully populated with short range 10G SFP+ transceivers of same OEM as NGFW from day 1 	
	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> 1x 1G/10G RJ45 management port from day 1. 	
High Availability Features	Active-Active and Active-Passive high availability features from day one. Each Box must come with full license.	
	Solution must have session failover for routing change, device and link failure monitoring functionality.	
	Proposed solution must support VRRP/HSRP or similar technology.	
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: Tap Mode, Transparent mode, Layer 2, Layer 3.	
Performance Capacity of Each NGFW appliance	Proposed appliance must have NGFW (FW + AVC + IPS) minimum performance of 65 Gbps in Multiprotocol / IMIX / Enterprise Mix environment with 1500/1518 bytes packet.	
	NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware, anti-spyware, Advance Threat, Zero day Protection and logging enabled with Minimum 25 Gbps.	
	Proposed appliance MUST support Connections Per Second – Minimum 385,000 or higher preferred.	
	Proposed appliance MUST support Concurrent Connection / Session – Minimum 18 Million or higher preferred.	
	All performance number mentioned in above clauses, must be available in public datasheet/Internal document .	
Advanced Routing	Support Multihop Ping and Multiple ISPs in Policy-Based Routing	
	Support Multihop Ping in Static Routes	
	Support BFD in Static Routes	

RESTRICTED

	Support OSPFv3 AH authentication for OSPFv3 protocol security.	
	Support IPv6 route aggregation	
	Support IPv4/IPv6 NAT-pool routes - Configure and redistribute NAT-pool routes to routing protocols.	
	Support PIM restart capability.	
	Support BGP for VxLAN interfaces.	
	Support Dynamic Routing support for GRE interfaces	
	Support for ECMP algorithms to provide traffic load balancing:	
	Support for DHCP Relay Agent Information Option 82	
	Support for OSPFv3 NSSA.	
	Support for IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.	
	Support for Routing Event Triggers to allow Cluster failover, and tearing down of BGP connections through monitored BGP and BFD sessions.	
	Support Routing Protocol History for BFD to improve troubleshooting capabilities.	
IPv6 Support	IPv6 support for L2, L3, Tap and Transparent mode operation	
	Should support on firewall policy with User and Applications	
	Should support SSL decryption on IPv6	
	Should support Stateless Address Auto configuration(SLAAC)	
Routing and Multicast support	Proposed firewall must support Static, OSPF (V2 & V3) and BGP routing protocols.	
	Policy-based forwarding	
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	
	Bidirectional Forwarding Detection (BFD)	
Authentication	Solution should support LDAP, TACACS+, Radius, Kerberos, Token-Based authentication protocols.	
	The proposed firewall's SSL VPN shall support LDAP, Radius, Kerberos, SAML, Token-Based etc. authentication protocols.	
	Proposed Solution must have capability to integrate with Active Directory from day 1. Solution should also be capable to impose Firewall Policy on AD User, Groups etc. from day 1.	
SSL/SSH Decryption and NAT Features	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.	
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.	
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well.	

RESTRICTED

	Proposed NGFW should support TLS Version 1.3 from day one.	
	The proposed firewall must be able to support Network Address Translation (NAT).	
	The proposed firewall must be able to support Port Address Translation (PAT).	
	The proposed firewall shall support Dual Stack IPv4 /IPv6 (NAT64, NPTv6).	
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription	
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.	
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP.	
	Proposed solution must support built-in IP address External Dynamic Lists to protect against malicious hosts.	
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.	
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User ID, Application and threat protection profile in firewall rule or the policy configuration.	
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application.	
	The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports.	
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or bad URLs.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in inbound and outbound connections.	
	The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.	
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first	
The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.		

RESTRICTED

	The Proposed firewall should support to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility.	
	The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.	
Intrusion Prevention System Features	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	
	IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
	IPS must support network exceptions based on source, destination, service or a combination of the three	
	IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts and generic attack types without predefined signatures	
	IPS must be able to collect packet capture for specific protections	
	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)	
	Vendor must supply evidence of leadership in protecting Microsoft vulnerabilities	
	IPS and/or Application Control must include the ability to detect and block P2P & evasive applications	
	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
	Solution must provide VOIP protocols protections	
	IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic	
Application Control and URL Filtering Requirements	Application control database must contain more than 6000 known applications.	
	Solution must have a URL categorization that exceeds 200 million URLs and covers more than 85% of Alexa's top 1M sites	
	Solution must be able to create a filtering rule with multiple categories	
	The Solution can inspect HTTPS based URL Filtering without requiring SSL decryption	
	Solution must be able to create a filtering for single site being supported by multiple categories.	
	Solution must have users and groups granularity with security rules	
	The security gateway local cache must give answers to 99% of URL categorization requests within 4 weeks in production	
	The solution must have an easy to use, searchable interface for applications and URLs	

RESTRICTED

	The solution must categorize applications and URLs and applications by Risk Factor	
	The application control and URLF security policy must be able to be defined by user identities	
	The application control and URLF database must be updated by a cloud based service	
	The solution must have unified application control and URLF security rules	
	The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy	
	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
	The solution must allow network exceptions based on defined network objects	
	The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page	
	Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category	
	Solution must provide an override mechanism on the categorization for the URL database	
Anti-Bot and Anti-Virus Feature Requirements	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	
	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	
	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	
	Anti-Bot protections must be able to scan for bot actions	
	The solution should support detection & prevention of Cryptors & ransomware viruses and variants (e.g. Wannacry, Cryptlocker , CryptoWall...) through use of static and/or dynamic analysis	
	The solution should have mechanisms to protect against spear phishing attacks	
	Look for C&C traffic patterns, not just at their DNS destination	
	Reverse engineer malware in order to uncover their DGA (Domain Name Generation)	
	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	
	The solution should have detection and prevention capabilities for DNS tunnelling attacks	
	Anti-Bot and Anti-Virus policy must be administered from a central console	
	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
	Anti-virus application must be able to prevent access to malicious websites	
	Anti-virus application must be able to inspect SSL encrypted traffic	

RESTRICTED

	Anti-Bot and Anti-Virus must be have real time updates from a cloud based reputation services	
	Anti-Virus must be able to stop incoming malicious files	
	Anti-Virus must be able to scan archive files	
	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement	
	The Anti-Virus should support scanning for links inside emails	
	The Anti-Virus should Scan files that are passing on CIFS protocol	
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years identically same for both the appliances.	
	The NGFW should be proposed with subscription licenses for L7 Application Control, Content Awareness, IPS, URL Filtering, Antivirus, Anti-Spam, Anti Bot, C&C Protection, DNS Security, Threat emulation, Threat extaction and Zero day protection for three (3) years identically same for both the appliances.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning, Deployment, Migration and Others	Vendor must offer required Professional Service (PS).	
	Professional Service Engineer will be responsible for following activity:	
	– Understanding procurement entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
– Post deployment knowledge sharing session with customer.		
	Working with procuring entity team for end-to-end UAT.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have Depo in Bangladesh and 24x7x365 Global TAC support	

24. WAN Firewall 2		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned by Bidder. (Preferably Checkpoint / Palo Alto)	

RESTRICTED

Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder	
No of WAN Firewall Units per Site	2 Units in HA	
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content / URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).	
3rd Party Test Certification	The offered hardware / model must maintain global standard certification for Safety, compliance and Environmental certificate. Vendor must mention certificate names.	
	The proposed OEM must be Leader in the latest Network Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof.	
	The protection rate of the proposed solution shall be 96% or above as per the latest published Enterprise Firewall Test Results from published by Cyber Rating. Reports to be submitted by the bidder as proof.	
General Security Features	The proposed solution shall provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic from day one	
	The proposed solution shall reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content from day one	
	The proposed solution shall prevent all known threats – Network DoS/DDoS, Malware, Spyware, Ransomware, Trojan, C&C, Malicious & Phishing Websites from day 1	
	The proposed solution shall Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior from day one	
	The proposed solution shall Inspect and control applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic from day one	
	All firewall must come with minimum 2 Virtual Contexts from day 1	
Storage	Proposed NGFW appliance must have 2 SSD and minimum 480 GB SSD of internal system storage.	
Memory (DRAM)	Minimum 128 GB RAM from day 1.	
Power	Full redundant Power Supplies from day 1.	

RESTRICTED

Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum	
	<ul style="list-style-type: none"> • 4x 1GE RJ45 ports from day 1 	
	The proposed NGFW appliance must have minimum	
	<ul style="list-style-type: none"> • 8x 1GE/10GE SFP and SFP+ ports/interfaces fully populated with short range 10G SFP+ transceivers of same OEM as NGFW from day 1 	
Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum	
	<ul style="list-style-type: none"> • 4x 10GE/25GE SFP+ and SFP28 compatible ports/interfaces fully populated with short range 25G Base transceiver of same OEM as NGFW from day 1. 	
	The proposed NGFW appliance must have minimum	
	<ul style="list-style-type: none"> • 1x 1Ge RJ45 purposeful dedicated HA port/interface from day 1. 	
High Availability Features	The proposed NGFW appliance must have minimum 1x 1G RJ45 management port from day 1.	
	Active-Active and Active-Passive high availability features from day one. Each Box must come with full license.	
	Solution must have session failover for routing change, device and link failure monitoring functionality.	
Interface Operation Mode	Proposed solution must support VRRP/HSRP or similar technology.	
	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: Tap Mode, Transparent mode, Layer 2, Layer 3.	
Performance Capacity of Each NGFW appliance	Proposed appliance must have NGFW (FW + AVC + IPS) minimum performance of 25 Gbps in Multiprotocol.	
	NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware, anti-spyware, Advance Threat, Zero day Protection and logging enabled with Minimum 16 Gbps.	
	Proposed appliance MUST support Connections Per Second – Minimum 240,000 or higher preferred.	
	Proposed appliance MUST support Concurrent Connection / Session – Minimum 4.5 Million or higher preferred.	
	All performance number mentioned in above clauses, must be available in public datasheet/Internal document .	
Advanced Routing	Support Multihop Ping and Multiple ISPs in Policy-Based Routing	
	Support Multihop Ping in Static Routes	
	Support BFD in Static Routes	
	Support OSPFv3 AH authentication for OSPFv3 protocol security.	
	Support IPv6 route aggregation	
	Support IPv4/IPv6 NAT-pool routes - Configure and redistribute NAT-pool routes to routing protocols.	
	Support PIM restart capability.	
	Support BGP for VxLAN interfaces.	
	Support Dynamic Routing support for GRE interfaces	
	Support for ECMP algorithms to provide traffic load balancing:	
	ISP Redundancy Extended supports for up to 10 ISP links.	
	Support for DHCP Relay Agent Information Option 82	

RESTRICTED

	Support for OSPFv3 NSSA.	
	Support for IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.	
	Support for Routing Event Triggers to allow Cluster failover, and tearing down of BGP connections through monitored BGP and BFD sessions.	
	Support Routing Protocol History for BFD to improve troubleshooting capabilities.	
IPv6 Support	IPv6 support for L2, L3, Tap and Transparent mode operation	
	Should support on firewall policy with User and Applications	
	Should support SSL decryption on IPv6	
	Should support Stateless Address Auto configuration(SLAAC)	
Routing and Multicast support	Proposed firewall must support Static, OSPF (V2 & V3) and BGP routing protocols.	
	Policy-based forwarding	
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	
	Bidirectional Forwarding Detection (BFD)	
Authentication	Solution should support LDAP, TACACS+, Radius, Kerberos, Token-Based authentication protocols.	
	The proposed firewall's SSL VPN shall support LDAP, Radius, Kerberos, SAML, Token-Based etc. authentication protocols.	
	Proposed Solution must have capability to integrate with Active Directory from day 1. Solution should also be capable to impose Firewall Policy on AD User, Groups etc. from day 1.	
SSL/SSH Decryption and NAT Features	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.	
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.	
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well.	
	Proposed NGFW should support TLS Version 1.3 from day one.	
	The proposed firewall must be able to support Network Address Translation (NAT).	
	The proposed firewall must be able to support Port Address Translation (PAT).	
	The proposed firewall shall support Dual Stack IPv4 /IPv6 (NAT64, NPTv6).	
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription	

RESTRICTED

Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.	
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP.	
	Proposed solution must support built-in IP address External Dynamic Lists to protect against malicious hosts.	
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.	
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User ID, Application and threat protection profile in firewall rule or the policy configuration.	
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application.	
	The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports.	
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or bad URLs.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in inbound and outbound connections.	
	The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.	
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first	
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.	
	The Proposed firewall should support to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility.	
The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.		
Intrusion Prevention	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	

RESTRICTED

System Features	IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
	IPS must support network exceptions based on source, destination, service or a combination of the three	
	IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts and generic attack types without predefined signatures	
	IPS must be able to collect packet capture for specific protections	
	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)	
	Vendor must supply evidence of leadership in protecting Microsoft vulnerabilities	
	IPS and/or Application Control must include the ability to detect and block P2P & evasive applications	
	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
	Solution must provide VOIP protocols protections	
	IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic	
Application Control and URL Filtering Requirements	Application control database must contain more than 6000 known applications.	
	Solution must have a URL categorization that exceeds 200 million URLs and covers more than 85% of Alexa's top 1M sites	
	Solution must be able to create a filtering rule with multiple categories	
	The Solution can inspect HTTPS based URL Filtering without requiring SSL decryption	
	Solution must be able to create a filtering for single site being supported by multiple categories.	
	Solution must have users and groups granularity with security rules	
	The security gateway local cache must give answers to 99% of URL categorization requests within 4 weeks in production	
	The solution must have an easy to use, searchable interface for applications and URLs	
	The solution must categorize applications and URLs and applications by Risk Factor	
	The application control and URLF security policy must be able to be defined by user identities	
	The application control and URLF database must be updated by a cloud based service	
	The solution must have unified application control and URLF security rules	

RESTRICTED

	The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy	
	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
	The solution must allow network exceptions based on defined network objects	
	The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page	
	Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category	
	Solution must provide an override mechanism on the categorization for the URL database	
Anti-Bot and Anti-Virus Feature Requirements	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	
	Anti-bot application must be able to detect and stop suspicious abnormal network behaviour	
	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	
	Anti-Bot protections must be able to scan for bot actions	
	The solution should support detection & prevention of Cryptors & ransomware viruses and variants (e.g. WannaCry, Crypt locker , CryptoWall...) through use of static and/or dynamic analysis	
	The solution should have mechanisms to protect against spear phishing attacks	
	Look for C&C traffic patterns, not just at their DNS destination	
	Reverse engineer malware in order to uncover their DGA (Domain Name Generation)	
	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	
	The solution should have detection and prevention capabilities for DNS tunnelling attacks	
	Anti-Bot and Anti-Virus policy must be administered from a central console	
	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
	Anti-virus application must be able to prevent access to malicious websites	
	Anti-virus application must be able to inspect SSL encrypted traffic	
	Anti-Bot and Anti-Virus must be have real time updates from a cloud based reputation services	
	Anti-Virus must be able to stop incoming malicious files	
	Anti-Virus must be able to scan archive files	
	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement	
The Anti-Virus should support scanning for links inside emails		

RESTRICTED

	The Anti-Virus should Scan files that are passing on CIFS protocol	
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years identically same for both the appliances.	
	The NGFW should be proposed with subscription licenses for L7 Application Control, Content Awareness, IPS, URL Filtering, Antivirus, Anti-Spam, Anti Bot, C&C Protection, DNS Security, Threat emulation, Threat extaction and Zero day protection for three (3) years identically same for both the appliances.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning, Deployment, Migration and Others	Vendor must offer required Professional Service (PS).	
	Professional Service Engineer will be responsible for following activity:	
	– Understanding procurement entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
– Post deployment knowledge sharing session with customer.		
	Working with procuring entity team for end-to-end UAT.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have Depo in Bangladesh and 24x7x365 Global TAC support	

25. DMZ Firewall 2		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned by the bidder. (Preferably Checkpoint / Palo Alto)	
Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder.	

RESTRICTED

No of DMZ Firewall Units per Site	2 Units in HA	
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content / URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).	
3rd Party Test Certification	The offered hardware / model must maintain global standard certification for Safety, compliance and Environmental certificate. Vendor must mention certificate names.	
	The proposed OEM must be Leader in the latest Network Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof.	
	The protection rate of the proposed solution shall be 96% or above as per the latest published Enterprise Firewall Test Results from published by Cyber Rating. Reports to be submitted by the bidder as proof.	
General Security Features	The proposed solution shall provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic from day one	
	The proposed solution shall reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content from day one	
	The proposed solution shall prevent all known threats – Network DoS/DDoS, Malware, Spyware, Ransomware, Trojan, C&C, Malicious & Phishing Websites from day 1	
	The proposed solution shall Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior from day one	
	The proposed solution shall Inspect and control applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic from day one	
	All firewall must come with minimum 2 Virtual Contexts from day 1	
Storage	Proposed NGFW appliance must have 2 SSD and minimum 480 GB SSD of internal system storage.	
Memory (DRAM)	Minimum 128 GB RAM from day 1.	
Power	Full redundant Power Supplies from day 1.	
Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> • 4x 1GE RJ45 ports from day 1 	
	The proposed NGFW appliance must have minimum <ul style="list-style-type: none"> • 8x 1GE/10GE SFP and SFP+ ports/interfaces fully populated with short range 10G SFP+ transceivers of same OEM as NGFW from day 1 	
	The proposed NGFW appliance must have minimum	

RESTRICTED

	<ul style="list-style-type: none"> 4x 10GE/25GE SFP+ and SFP28 compatible ports/ interfaces fully populated with short range 25G Base transceiver of same OEM as NGFW from day 1. 	
	<p>The proposed NGFW appliance must have minimum</p> <ul style="list-style-type: none"> 1x 1Ge RJ45 purposeful dedicated HA port/interface from day 1. 	
	<p>The proposed NGFW appliance must have minimum</p> <ul style="list-style-type: none"> 1x 1G RJ45 management port from day 1. 	
High Availability Features	Active-Active and Active-Passive high availability features from day one. Each Box must come with full license.	
	Solution must have session failover for routing change, device and link failure monitoring functionality.	
	Proposed solution must support VRRP/HSRP or similar technology.	
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: Tap Mode, Transparent mode, Layer 2, Layer 3.	
Performance Capacity of Each NGFW appliance	Proposed appliance must have NGFW (FW + AVC + IPS) minimum performance of 25 Gbps in Multiprotocol.	
	NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware, anti-spyware, Advance Threat, Zero day Protection and logging enabled with Minimum 16 Gbps.	
	Proposed appliance MUST support Connections Per Second – Minimum 240,000 or higher preferred.	
	Proposed appliance MUST support Concurrent Connection / Session – Minimum 4.5 Million or higher preferred.	
	All performance number mentioned in above clauses, must be available in public datasheet/Internal document .	
Advanced Routing	Support Multihop Ping and Multiple ISPs in Policy-Based Routing	
	Support Multihop Ping in Static Routes	
	Support BFD in Static Routes	
	Support OSPFv3 AH authentication for OSPFv3 protocol security.	
	Support IPv6 route aggregation	
	Support IPv4/IPv6 NAT-pool routes - Configure and redistribute NAT-pool routes to routing protocols.	
	Support PIM restart capability.	
	Support BGP for VxLAN interfaces.	
	Support Dynamic Routing support for GRE interfaces	
	Support for ECMP algorithms to provide traffic load balancing;	
	ISP Redundancy Extended supports for up to 10 ISP links.	
	Support for DHCP Relay Agent Information Option 82	
	Support for OSPFv3 NSSA.	
	Support for IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.	
Support for Routing Event Triggers to allow Cluster failover, and tearing down of BGP connections through monitored BGP and BFD sessions.		

RESTRICTED

	Support Routing Protocol History for BFD to improve troubleshooting capabilities.	
IPv6 Support	IPv6 support for L2, L3, Tap and Transparent mode operation	
	Should support on firewall policy with User and Applications	
	Should support SSL decryption on IPv6	
	Should support Stateless Address Auto configuration(SLAAC)	
Routing and Multicast support	Proposed firewall must support Static, OSPF (V2 & V3) and BGP routing protocols.	
	Policy-based forwarding	
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	
	Bidirectional Forwarding Detection (BFD)	
Authentication	Solution should support LDAP, TACACS+, Radius, Kerberos, Token-Based authentication protocols.	
	The proposed firewall's SSL VPN shall support LDAP, Radius, Kerberos, SAML, Token-Based etc. authentication protocols.	
	Proposed Solution must have capability to integrate with Active Directory from day 1. Solution should also be capable to impose Firewall Policy on AD User, Groups etc. from day 1.	
SSL/SSH Decryption and NAT Features	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.	
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.	
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well.	
	Proposed NGFW should support TLS Version 1.3 from day one.	
	The proposed firewall must be able to support Network Address Translation (NAT).	
	The proposed firewall must be able to support Port Address Translation (PAT).	
	The proposed firewall shall support Dual Stack IPv4 /IPv6 (NAT64, NPTv6).	
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription	
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.	
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP.	
	Proposed solution must support built-in IP address External Dynamic Lists to protect against malicious hosts.	
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture	

RESTRICTED

	feature of the firewall without any third-party tool or technical support.	
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User ID, Application and threat protection profile in firewall rule or the policy configuration.	
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application.	
	The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports.	
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or bad URLs.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in inbound and outbound connections.	
	The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.	
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first	
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.	
	The Proposed firewall should support to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility.	
	The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.	
Intrusion Prevention System Features	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	
	IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
	IPS must support network exceptions based on source, destination, service or a combination of the three	
	IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts and generic attack types without predefined signatures	
	IPS must be able to collect packet capture for specific protections	

RESTRICTED

	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)	
	Vendor must supply evidence of leadership in protecting Microsoft vulnerabilities	
	IPS and/or Application Control must include the ability to detect and block P2P & evasive applications	
	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
	Solution must provide VOIP protocols protections	
	IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic	
Application Control and URL Filtering Requirements	Application control database must contain more than 6000 known applications.	
	Solution must have a URL categorization that exceeds 200 million URLs and covers more than 85% of Alexa's top 1M sites	
	Solution must be able to create a filtering rule with multiple categories	
	The Solution can inspect HTTPS based URL Filtering without requiring SSL decryption	
	Solution must be able to create a filtering for single site being supported by multiple categories.	
	Solution must have users and groups granularity with security rules	
	The security gateway local cache must give answers to 99% of URL categorization requests within 4 weeks in production	
	The solution must have an easy to use, searchable interface for applications and URLs	
	The solution must categorize applications and URLs and applications by Risk Factor	
	The application control and URLF security policy must be able to be defined by user identities	
	The application control and URLF database must be updated by a cloud based service	
	The solution must have unified application control and URLF security rules	
	The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy	
	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
	The solution must allow network exceptions based on defined network objects	
	The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page	
Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category		
Solution must provide an override mechanism on the categorization for the URL database		

RESTRICTED

Anti-Bot and Anti-Virus Feature Requirements	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	
	Anti-bot application must be able to detect and stop suspicious abnormal network behaviour	
	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	
	Anti-Bot protections must be able to scan for bot actions	
	The solution should support detection & prevention of Cryptors & ransomware viruses and variants (e.g. Wannacry, Cryptlocker , CryptoWall...) through use of static and/or dynamic analysis	
	The solution should have mechanisms to protect against spear phishing attacks	
	Look for C&C traffic patterns, not just at their DNS destination	
	Reverse engineer malware in order to uncover their DGA (Domain Name Generation)	
	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	
	The solution should have detection and prevention capabilities for DNS tunneling attacks	
	Anti-Bot and Anti-Virus policy must be administered from a central console	
	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
	Anti-virus application must be able to prevent access to malicious websites	
	Anti-virus application must be able to inspect SSL encrypted traffic	
	Anti-Bot and Anti-Virus must be have real time updates from a cloud based reputation services	
	Anti-Virus must be able to stop incoming malicious files	
	Anti-Virus must be able to scan archive files	
	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement	
	The Anti-Virus should support scanning for links inside emails	
The Anti-Virus should Scan files that are passing on CIFS protocol		
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years identically same for both the appliances.	
	The NGFW should be proposed with subscription licenses for L7 Application Control, Content Awareness, IPS, URL Filtering, Antivirus, Anti-Spam, Anti Bot, C&C Protection, DNS Security, Threat emulation, Threat extraction and Zero day protection for three (3) years identically same for both the appliances.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning,	Vendor must offer required Professional Service (PS).	
	Professional Service Engineer will be responsible for following activity:	

RESTRICTED

Deployment, Migration and Others	– Understanding procurement entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
	– Post deployment knowledge sharing session with customer.	
	Working with procuring entity team for end-to-end UAT.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have Depo in Bangladesh and 24x7x365 Global TAC support	

26. Branch Firewall Type-1		
Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by Bidder. (Preferably Checkpoint / Cisco / Palo Alto)	
Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder.	
Architecture	The NGFW architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions like configuration, reporting and route update & Data Plane should handle Signature matching (like exploits, virus, spyware), Security processing (like apps, users, content / URL, policy match, SSL decryption, app decoding etc) & Network Processing (like flow control, route lookup, MAC lookup, QoS, NAT etc).	
3rd Party Test Certification	The offered hardware / model must maintain global standard certification for Safety, compliance and Environmental certificate. Vendor must mention certificate names.	
	The proposed OEM must be Leader in the latest Network Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof.	
	The protection rate of the proposed solution shall be 96% or above as per the latest published Enterprise Firewall Test Results from published by Cyber Rating. Reports to be submitted by the bidder as proof.	
General Security Features	The proposed solution shall provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic from day one	
	The proposed solution shall reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content from day one	
	The proposed solution shall prevent all known threats – Network DoS/DDoS, Malware, Spyware, Ransomware, Trojan, C&C, Malicious & Phishing Websites from day 1	
	The proposed solution shall Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior from day one	
	The proposed solution shall Inspect and control applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic from day one	
	All firewall must come with minimum 2 Virtual Contexts from day 1	

RESTRICTED

Storage	Proposed NGFW appliance must have 1 SSD and minimum 240 GB SSD of internal system storage.	
Memory (DRAM)	Minimum 16 GB RAM from day 1.	
Power	Full redundant Power Supplies from day 1.	
Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum 4x 1GE RJ45 ports from day 1	
	The proposed NGFW appliance must have minimum 1x 1G RJ45 management port from day 1.	
High Availability Features	Active-Active and Active-Passive high availability features.	
	Solution must have session failover for routing change, device and link failure monitoring functionality.	
	Proposed solution must support VRRP/HSRP or similar technology.	
Interface Operation Mode	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: Tap Mode, Transparent mode, Layer 2, Layer 3.	
Performance Capacity of Each NGFW appliance	Proposed appliance must have NGFW (FW + AVC + IPS) minimum performance of 2.5 Gbps in Multiprotocol / IMIX / Enterprise Mix environment with 1500/1518 bytes packet.	
	NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware, anti-spyware, Advance Threat, Zero day Protection and logging enabled with Minimum 1.4 Gbps.	
	Proposed appliance MUST support Connections Per Second – Minimum 55,000 or higher preferred.	
	Proposed appliance MUST support Concurrent Connection / Session – Minimum 3.7 Million or higher preferred.	
	All performance number mentioned in above clauses, must be available in public datasheet/Internal document .	
Advanced Routing	Support Multihop Ping and Multiple ISPs in Policy-Based Routing	
	Support Multihop Ping in Static Routes	
	Support BFD in Static Routes	
	Support OSPFv3 AH authentication for OSPFv3 protocol security.	
	Support IPv6 route aggregation	
	Support IPv4/IPv6 NAT-pool routes - Configure and redistribute NAT-pool routes to routing protocols.	
	Support PIM restart capability.	
	Support BGP for VxLAN interfaces.	
	Support Dynamic Routing support for GRE interfaces	
	Support for ECMP algorithms to provide traffic load balancing:	
	ISP Redundancy Extended supports for up to 10 ISP links.	
	Support for DHCP Relay Agent Information Option 82	

RESTRICTED

	Support for OSPFv3 NSSA.	
	Support for IPv6 Static MFC Cache to enable forwarding of multicast data without PIM configuration.	
	Support for Routing Event Triggers to allow Cluster failover, and tearing down of BGP connections through monitored BGP and BFD sessions.	
	Support Routing Protocol History for BFD to improve troubleshooting capabilities.	
IPv6 Support	IPv6 support for L2, L3, Tap and Transparent mode operation	
	Should support on firewall policy with User and Applications	
	Should support SSL decryption on IPv6	
	Should support Stateless Address Auto configuration(SLAAC)	
Routing and Multicast support	Proposed firewall must support Static, OSPF (V2 & V3) and BGP routing protocols.	
	Policy-based forwarding	
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	
	Bidirectional Forwarding Detection (BFD)	
Authentication	Solution should support LDAP, TACACS+, Radius, Kerberos, Token-Based authentication protocols.	
	The proposed firewall's SSL VPN shall support LDAP, Radius, Kerberos, SAML, Token-Based etc. authentication protocols.	
	Proposed Solution must have capability to integrate with Active Directory from day 1. Solution should also be capable to impose Firewall Policy on AD User, Groups etc. from day 1.	
SSL/SSH Decryption and NAT Features	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an inbound connection.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.	
	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic.	
	SSL decryption must be supported on any port used for SSL i.e. SSL decryption must be supported on non-standard SSL port as well.	
	Proposed NGFW should support TLS Version 1.3 from day one.	
	The proposed firewall must be able to support Network Address Translation (NAT).	
	The proposed firewall must be able to support Port Address Translation (PAT).	
	The proposed firewall shall support Dual Stack IPv4 /IPv6 (NAT64, NPTv6).	

RESTRICTED

	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription	
Next Generation Firewall Features	The proposed firewall shall have network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic.	
	The proposed firewall shall be able to handle (alert, block or allow) unknown / unidentified applications like unknown UDP & TCP.	
	Proposed solution must support built-in IP address External Dynamic Lists to protect against malicious hosts.	
	The proposed firewall shall be able to create custom application signatures and categories using the inline packet capture feature of the firewall without any third-party tool or technical support.	
	The proposed firewall shall be able to implement Zones, IP address, Port numbers, User ID, Application and threat protection profile in firewall rule or the policy configuration.	
	The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application.	
	The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports.	
	The proposed firewall shall be able to protect the user from the malicious content upload or download by application such as Facebook chat or file sharing by enforcing the total threat protection for known and unknown malicious content such as virus, malware or bad URLs.	
	The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in inbound and outbound connections.	
	The proposed firewall shall be able to identify port-based rules/policies so admin / security team can convert them to application-based whitelist rules or add applications to existing rules without compromising application availability.	
	The proposed firewall shall be able to identifies the rules configured with unused applications and prioritize which rules to migrate or clean up first	
	The proposed firewall shall be able restrict application traffic to its default ports to prevent evasive applications from running on non-standard ports.	
The Proposed firewall should support to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility.		

RESTRICTED

	The NGFW must support the ability to dynamically and automatically regroup user/s based on security events relating to that user, no manual response needed.	
Intrusion Prevention System Features	IPS must be based on the following detection mechanisms: exploit signatures, protocol anomalies, application controls and behavior-based detection	
	IPS must have a software based fail-open mechanism, configurable based on thresholds of security gateways CPU and memory usage	
	IPS must support network exceptions based on source, destination, service or a combination of the three	
	IPS must be able to detect and prevent the following threats: Protocol misuse, malware communications, tunneling attempts and generic attack types without predefined signatures	
	IPS must be able to collect packet capture for specific protections	
	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP, Windows services (Microsoft Networking)	
	Vendor must supply evidence of leadership in protecting Microsoft vulnerabilities	
	IPS and/or Application Control must include the ability to detect and block P2P & evasive applications	
	Solution must protect from DNS Cache Poisoning, and prevents users from accessing blocked domain addresses	
	Solution must provide VOIP protocols protections	
IPS and/or Application Control must detect and block remote controls applications, including those that are capable tunneling over HTTP traffic		
Application Control and URL Filtering Requirements	Application control database must contain more than 6000 known applications.	
	Solution must have a URL categorization that exceeds 200 million URLs and covers more than 85% of Alexa's top 1M sites	
	Solution must be able to create a filtering rule with multiple categories	
	The Solution can inspect HTTPS based URL Filtering without requiring SSL decryption	
	Solution must be able to create a filtering for single site being supported by multiple categories.	
	Solution must have users and groups granularity with security rules	
	The security gateway local cache must give answers to 99% of URL categorization requests within 4 weeks in production	
	The solution must have an easy to use, searchable interface for applications and URLs	
	The solution must categorize applications and URLs and applications by Risk Factor	

RESTRICTED

	The application control and URLF security policy must be able to be defined by user identities	
	The application control and URLF database must be updated by a cloud based service	
	The solution must have unified application control and URLF security rules	
	The solution must provide a mechanism to inform or ask users in real time to educate them or confirm actions based on the security policy	
	The solution must provide a mechanism to limit application usage based on bandwidth consumption	
	The solution must allow network exceptions based on defined network objects	
	The solution must provide the option to modify the Blocking Notification and to redirect the user to a remediation page	
	Solution must include a Black and White lists mechanism to allow the administrator to deny or permit specific URLs regardless of the category	
	Solution must provide an override mechanism on the categorization for the URL database	
Anti-Bot and Anti-Virus Feature Requirements	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	
	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	
	Anti-Bot application must use a multi-tiered detection engine, which includes the reputation of IPs, URLs and DNS addresses and detect patterns of bot communications	
	Anti-Bot protections must be able to scan for bot actions	
	The solution should support detection & prevention of Cryptors & ransomware viruses and variants (e.g. Wannacy, Cryptlocker , CryptoWall...) through use of static and/or dynamic analysis	
	The solution should have mechanisms to protect against spear phishing attacks	
	Look for C&C traffic patterns, not just at their DNS destination	
	Reverse engineer malware in order to uncover their DGA (Domain Name Generation)	
	DNS trap feature as part of our threat prevention, assisting in discovering infected hosts generating C&C communication	
	The solution should have detection and prevention capabilities for DNS tunneling attacks	
	Anti-Bot and Anti-Virus policy must be administered from a central console	
	Anti-Bot and Anti-Virus application must have a centralized event correlation and reporting mechanism	
	Anti-virus application must be able to prevent access to malicious websites	

RESTRICTED

	Anti-virus application must be able to inspect SSL encrypted traffic	
	Anti-Bot and Anti-Virus must be have real time updates from a cloud based reputation services	
	Anti-Virus must be able to stop incoming malicious files	
	Anti-Virus must be able to scan archive files	
	Anti-Virus and Anti-Bot policies must be centrally managed with granular policy configuration and enforcement	
	The Anti-Virus should support scanning for links inside emails	
	The Anti-Virus should Scan files that are passing on CIFS protocol	
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years identically same for both the appliances.	
	The NGFW should be proposed with subscription licenses for L7 Application Control, Content Awareness, IPS, URL Filtering, Antivirus, Anti-Spam, Anti Bot, C&C Protection, DNS Security, Threat emulation, Threat extaction and Zero day protection for three (3) years.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning, Deployment, Migration and Others	Vendor must offer required Professional Service (PS).	
	Professional Service Engineer will be responsible for following activity:	
	– Understanding procurement entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
	– Post deployment knowledge sharing session with customer.	
	Working with procuring entity team for end-to-end UAT.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have Depo in Bangladesh and 24x7x365 Global TAC support	

27. Branch Firewall Type-2		
Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Country of Origin	As per tender specification, article 20	
Country of Manufacturing	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 1 RU	
Industry Certifications and Evaluations	The proposed solution must be positioned as a Leader in the Enterprise Firewalls segment of the latest Forrester Wave or Gartner Magic Quadrant.	
Part No	Bidder Must submit BOQ of proposed device including the details part numbers and Manufacturer Warranty. The bidder should submit the required performance document for the proposed device.	
Hardware Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory and should support a minimum of 16 GB of RAM.	
	The appliance should support at least 8x1G Copper ports & 2x10G SFP+ ports from day 1.	
	The proposed firewall solution should have at least 8 core CPU.	
	The proposed firewall should have at least 400 GB of storage from day 1.	
	Should support Active-Standby high availability from day one	
Performance & Scalability	Must have at least 8.5 Gbps Next Generation Intrusion Prevention system (IPS) Throughput	
	Must have at least 8.8 Gbps Firewall with (AVC) Throughput	
	NG Firewall Must support at least 280K concurrent sessions with AVC	
	NG Firewall Must support at least 45k new connections per second with AVC or 240k layer 4 new session per second	
	NG Firewall Must support at least 9 Gbps IPsec VPN Throughput	
	NG Firewall Must support at least Maximum VPN Peers 280 or more.	
NGFW Features	Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple	

RESTRICTED

	activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. This feature is extremely important for organization to build capabilities to identify internal attacks and malicious connections. Bidder must propose next-generation firewall with intrusion prevention system (IPS), malware and Spyware protection and application detection feature.	
	Firewall Must support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, zones, vlan, etc	
	Must support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance. Each instance Must have its own OS & can shutdown/restart an instance when needed	
	Firewall Must support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat which must be from day 1 (not in license based).	
	Firewall Must support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
	The solution Must support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
	The solution Must support Multicast protocols like IGMP, PIM, etc	
	Must support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Must be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Must be capable of detecting and blocking IPv6 attacks.	
	Must support more than 30,000 (excluding custom signatures) IPS signatures or more. Must support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	Must support at-least 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and Must be able to create 60 or more application categories for operational efficiency	
	The Appliance OEM must have its own threat intelligence analysis center and Must use the global footprint of security deployments for more comprehensive network protection.	

RESTRICTED

	The detection engine Must support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.)	
	The detection engine Must support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
	Must support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
	Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance. Bidder can propose multiple appliance / higher chassis to meet the solution requirement.	
	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
URL Filtering Features	Should must support URL threat intelligence feeds to protect against threats	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	
	Should support safe search for YouTube EDU enforcement	
Anti-APT / Malware Features	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
	Proposed solution shall have required subscription like Threat Intelligence for proper functioning	
Design and Implementation Scope	Bidder Must submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	
	Bidder must submit the required performance document and compliance reference document for the proposed device.	

RESTRICTED

	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to IT Division.	
Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning with consultation with IT Department.	
Licenses	The NGFW must be proposed with 3(Three) Years subscription licenses for URL filtering, Advanced Malware Protection with cloud sandboxing facilities, IPS, and Centralized Management System licenses.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

28. Branch Firewall 3		
Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by Bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 1 RU	
Industry Certifications and Evaluations	The proposed solution must be positioned as a Leader in the Enterprise Firewalls segment of the latest Forrester Wave or Gartner Magic Quadrant.	
Part No	Bidder Must submit BOQ of proposed device including the details part numbers and Manufacturer Warranty. The bidder should submit the required performance document for the proposed device.	
Hardware Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to	

RESTRICTED

	support higher memory and should support a minimum of 16 GB of RAM.	
	The appliance should support at least 8x1G Copper ports from day 1.	
	The proposed firewall solution should have at least 8 core CPU.	
	The proposed firewall should have at least 400 GB of storage from day 1.	
	Should support Active-Standby high availability from day one	
Performance & Scalability	Must have at least 5.5 Gbps Next Generation Intrusion Prevention system (IPS) Throughput	
	Must have at least 6 Gbps Firewall with (AVC) Throughput	
	NG Firewall Must support at least 190K concurrent sessions with AVC	
	NG Firewall Must support at least 30k new connections per second with AVC or 160k layer 4 new session per second	
	NG Firewall Must support at least 4.8 Gbps IPSec VPN Throughput	
	NG Firewall Must support at least Maximum VPN Peers 180 or more.	
NGFW Features	Solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. This feature is extremely important for organization to build capabilities to identify internal attacks and malicious connections. Bidder must propose next-generation firewall with intrusion prevention system (IPS), malware and Spyware protection and application detection feature.	
	Firewall Must support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, zones, vlan, etc	
	Must support capability to create multiple virtual context/instance with strict hardware resource (CPU, Memory & Storage) reservation and ensure traffic isolation between virtual context/instance. Each instance Must have its own OS & can shutdown/restart an instance when needed	
	Firewall Must support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat which must be from day 1 (not in license based).	
	Firewall Must support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
	The solution Must support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	

RESTRICTED

	The solution Must support Multicast protocols like IGMP, PIM, etc	
	Must support capability to integrate with other security solutions to receive contextual information like security group tags/names	
	Must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
	Must be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
	Must be capable of detecting and blocking IPv6 attacks.	
	Must support more than 30,000 (excluding custom signatures) IPS signatures or more. Must support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy	
	Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
	Must support at-least 6000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and Must be able to create 60 or more application categories for operational efficiency	
	The Appliance OEM must have its own threat intelligence analysis center and Must use the global footprint of security deployments for more comprehensive network protection.	
	The detection engine Must support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.)	
	The detection engine Must support the capability of detecting variants of known threats, as well as new threats	
	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	
	Must support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
	Must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network and capability to do dynamic analysis on premise (if required in future) on purpose built-appliance. Bidder can propose multiple appliance / higher chassis to meet the solution requirement.	

RESTRICTED

	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
URL Filtering Features	Should must support URL threat intelligence feeds to protect against threats	
	Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than 280 million of URLs in more than 80 categories.	
	Should support safe search for YouTube EDU enforcement	
Anti-APT / Malware Features	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
	Proposed solution shall have required subscription like Threat Intelligence for proper functioning	
Design and Implementation Scope	Bidder Must submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	
	Bidder must submit the required performance document and compliance reference document for the proposed device.	
	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to IT Division.	
Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning with consultation with IT Department.	
Licenses	The NGFW must be proposed with 3(Three) Years subscription licenses for URL filtering, Advanced Malware Protection with cloud sandboxing facilities , IPS, and Centralized Management System licenses.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

29. Industry Grade Firewall for Ship

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by the bidder.	
Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder.	
No of Rugged Firewall Units per Site	1	
3rd Party Test Certification	<p>The offered hardware / model must maintain global standard certification to Operate in Harsh Conditions and should be clearly mentioned in</p> <p>i) published data sheet of offered NGFW. IEEE 1613 , IEC 61850-3 , IEC 60945, EN/IEC 60529, heat and immunity to electromagnetic interference.</p> <p>ii) EN/IEC 60529 , IEC 60068-2-27 shock, IEC 60068-2-6 vibration.</p> <p>iii) IEC-60945 B, DNV-GL-CG-0339</p> <p>iv) IP30</p> <p>v) Operating Temperature Range: -40°C ~ 75°C (-40°F ~ 167°F)</p>	
	The proposed OEM must be Leader in the latest Network Firewall Gartner Magic Quadrant for last consecutive three years. Reports to be submitted by the bidder as proof.	
	The protection rate of the proposed solution shall be 96% or above as per the latest published Enterprise Firewall Test Results from published by Cyber Rating. Reports to be submitted by the bidder as proof.	
General Security Features	The proposed solution shall provide complete visibility of Network, all applications (including cloud & SaaS), all users and devices (including all locations) and encrypted traffic from day one	
	The proposed solution shall reduce attack surface area by enabling business apps, block 'bad' apps, Limit application functions, limit high risk websites and content from day one	
	The proposed solution shall prevent all known threats – Network DoS/DDoS, Malware, Spyware, Ransomware, Trojan, C&C, Malicious & Phishing Websites from day 1	
	The proposed solution shall Detect and prevent new threats – unknown malware, zero-day exploits and custom attack behavior from day one	
	The proposed solution shall Inspect and control applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic from day one	

RESTRICTED

Power	Industrial Grade Power Supplies with operating temperature range of (-40° ~ 70°C, -40° ~ 158°F) from day 1.	
Interface Requirement of Each NGFW appliance	The proposed NGFW appliance must have minimum 2x 1GE copper/SFP (Combo) ports from day 1	
	The proposed NGFW appliance must have minimum 4x 1GE RJ45 ports from day 1.	
	The proposed NGFW appliance must have minimum 1x 1G RJ45 serial console port from day 1.	
High Availability Features	The proposed solution shall have high availability feature.	
Performance Capacity of Each NGFW appliance	Proposed appliance must have NGFW (FW + AVC + IPS) minimum performance of 790 Mbps.	
	NG Threat prevention throughput in real world/production environment (by enabling and measured with application control, IPS, antivirus, Anti malware, anti-spyware, Advance Threat, Zero day Protection and logging enabled with Minimum 390 Mbps.	
	Proposed appliance MUST support Connections Per Second – Minimum 13500 or higher preferred.	
	Proposed appliance MUST support Concurrent Connection / Session – Minimum 0.9 Million or higher preferred.	
	All performance number mentioned in above clauses, must be available in public datasheet/Internal document .	
IPv6 Support	IPv6 support for L2, L3 and Transparent mode operation	
	Should support on firewall policy with User and Applications	
Routing and Multicast support	Proposed firewall must support Static, OSPF (V2) and BGP routing protocols.	
	Policy-based forwarding	
	PIM-SM, PIM-SSM, IGMP v1, v2, and v3.	
Authentication	Solution should support LDAP, TACACS+, Radius, Kerberos, Token-Based authentication protocols.	
	The proposed firewall's SSL VPN shall support LDAP, Radius, Kerberos, SAML, Token-Based etc. authentication protocols.	
	Proposed Solution must have capability to integrate with Active Directory from day 1. Solution should also be capable to impose Firewall Policy on AD User, Groups etc. from day 1.	
NAT Features	The proposed firewall must be able to support Network Address Translation (NAT).	
	The proposed firewall must be able to support Port Address Translation (PAT).	
	The proposed firewall shall support Dual Stack IPv4 /IPv6 (NAT64, NPTv6).	
	Should support Dynamic IP reservation, tunable dynamic IP and port over subscription	
Specific Features	The proposed solution shall have the following features from day 1	

RESTRICTED

	Next Generation Firewall	
	Site-to-Site VPN	
	Remote Access VPN	
	Application Control and Web Filtering	
	Intrusion Prevention (IPS)	
	Antivirus	
	Threat Emulation	
	Protection against unpatched systems or systems running on legacy operating systems and software which don't have the updated patch/es due to unavoidable circumstances.	
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years.	
	The NGFW should be proposed with subscription licenses for L7 Application Control, Content Awareness, IPS, URL Filtering, Antivirus, Anti-Spam, Anti Bot, C&C Protection, DNS Security, Threat emulation and Zero day protection for three (3) years identically same for both the appliances.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning, Deployment, Migration and Others	Vendor must offer required Professional Service (PS).	
	Professional Service Engineer will be responsible for following activity:	
	– Understanding procurement entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
– Post deployment knowledge sharing session with customer.		
	Working with procuring entity team for end-to-end UAT.	

30: Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security		
Items	Required Technical Specifications	Bidder's Response
Brand	Internationally reputed brand. (Preferably F5)	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Manufacturing Country	As per tender specification, article 20	
Solution Architecture Requirement	The proposed solution have to perform as a dedicated appliance-based Next Generation Anti-DDOS, DNS and GSLB Solution also run on the same hardware platform. Relevant solutions should be scalable with the same Hardware platform. On premised solution should support integrate with cloud Anti-DDOS scrubbing system for DDoS mitigation and clean traffic. The proposed hardware appliance management OS should be containerized platform based modern architecture and Multi-tenancy platform OS.	
	The solution must support both Forward Proxy and Reverse proxy mode as a full proxy (Forward Proxy & Reverse Proxy) architecture to control separate user sessions and separate application sessions on ingress and egress point for more control and complete visibility of security on layer 3 to Layer 7.	
	Proposed device must support multi-tenancy with partitions based on purpose-built isolation mechanism of the tenants at the device level. The proposed solution should support minimum 8 tenants / guests in isolated environments from day -1 and it support upgradation up to 26 tenants in future without changing hardware.	
Management System	The entire solution should support integration with central management system to centrally manage Anti-DDOS policies for day to day operations from single console.	
	Management Port : 1x 1000BASE-T,1x USB 3.0,1x serial console	
	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot or on device packet captures on appliance config and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link.	
Appliance Resource	The appliance should have minimum 128 GB DDR memory or higher.	
	The appliance should have minimum one 1TB SSD drives or higher	
	The proposed system must have redundant power supply from Day 1.	
	The proposed hardware appliance must be 1U rackmountable hardware appliance.	

RESTRICTED

	<p>The proposed solution should have minimum</p> <ul style="list-style-type: none"> • 8 x 25G/10G SFP28/SFP+ ports • 2 x 100G/40G QSFP+/QSFP28 ports from day 1. <p>Bidder has to propose 8 x 10 GE SR SFP+ for each appliance. All the SFP module should be same OEM original SFP.</p>	
	The solution must have High Availability for both TCP session mirroring and SSL session mirroring in full-proxy (Forward Proxy and Reverse Proxy) mode in Active-Standby HA Architecture.	
	The proposed appliance should support L4 throughput of 95 Gbps or higher	
	The proposed appliance should support minimum 75 Million L4 concurrent connections from day 1 and upgradeable up to 100Million without changing the hardware platform if required in future.	
	The proposed appliance should support minimum 80M SYN cookies per second of HW DDoS protection from day 1.	
	The proposed appliance should support 35 Gbps of SSL based hardware offloading throughput from day1 and upgradeable up to 50 Gbps on the same hardware platform in future.	
	The SSL encryption & decryption process must be hardware-based processor for acceleration.	
	The proposed appliance must support minimum 60K SSL TPS (2K SSL) from day 1 and upgradeable up to 100K TPS on same hardware platform in future.	
	6vCPU Reserved for Control Plane OS and 12 vCPU's Available for Multi-Tenancy and Data-plane from Day 1. It can be upgradeable up to 26 vCPU's for Multi-Tenancy on the same hardware platform in future.	
	The Proposed solution should have multi tenancy capability within the same appliance, where tenancy consist with dedicated OS, vCPU, RAM and storage along with tenant wise administrative priviledge.	
	The proposed solution should allows for configuration of up to 2000 virtual route segment or VRF on proposed solution that support Layer 3 virtualization, traffic segmentation, routing isolation for traffic security within the tenant.	
	The proposed solution must have multiple license provision option within One tenant and also all the licenses must be shareable within the all of the tenants on the same appliance.	
Protction from DNS based DDOS and flooding attacks	The proposed solution support Domain Name System features including DNS Protection and DNS-based Global Server Load Balancing.	
	Solution should support Network-wide protections:	
	Connection limit per source IP, dynamic backlisting per source IP violating the threshold.	
	Inbound and outbound threat protection	

RESTRICTED

	DNS Flood Protection: The proposed solution should detect statistical anomalies in DNS traffic and mitigate DNS floods using following mechanism	
	DNS query limit	
	DNS Domain attack protection	
	DNS TCP active authentication mechanism	
	DNS regular expression	
	DNS Cache Poisoning	
Authoritative DNS Feature Requirements	Solution must have standards-based DNS services for GSLB / DNS.	
	Solution must support 1000 DNS Request Per Second (RPS) from day 1 and scalable to 2.7 M DNS Request Per Second (RPS) in future if required.	
	The solution must support IP Anycast for DNS	
	Authoritative Name Servers should have the built-in protection using DNS Response Rate limiting	
	The DNS solution must have traffic steering like Load Balancing and Global Server Load Balancing	
	The DNS solution must have IPv6 & IPv4 Dual stack Compliant including all NAT requirements & DNSSEC requirements.	
	Able to support mixed combinations of IPv6 and IPv4 virtual addresses and nodes resolving AAAA queries without requiring wholesale network and application upgrades. This provides DNS gateway and translation services for hybrid IPv6 and IPv4 solutions and manages IPv6 and IPv4 DNS servers in DNS64 environments.	
	Deliver high speed standard (non-GSLB) DNS query responses. E.g. addressing queries at very high speed by obtaining configuration via zone transfer from primary authoritative DNS Servers and accommodate large numbers of zones and records.	
Should have Hardware Acceleration for DNS Caching and able to cache DNS responses		
DNSSEC and other Security Feature Requirement	The solution must support the standard DNSSEC specifications	
	Provide flexibility to implement DNS filtering, query logging, and other DNS firewall user cases to limit or deny websites access based on source, destination, or port	
	The DNS solution should support to intercept event when DNS request, DNS response and DNS returns for granular DNS traffic control.	
	The DNS solution should support Hyper-scale Service Responses and absorb DNS DDoS.	
	The DNS Solution should support DNS over HTTPS, DNS over TLS and Proxying DNS over HTTPS Queries to Traditional DNS Servers.	
	The DNS solution should able to provide IP Anycast integration to increase DNS performance as more devices are added to support millions of DNS queries. DNS query volumes directed to one IP Address, whether legitimate or	

	during a denial of service attack, are easily managed by distributing the load among multiple geographic devices	
	The DNS should use Secure methods for data updates between the devices in the system.	
	DNS solution should be ICSA Labs certified as a firewall and resists common teardrop, ICMP, and daemon attacks.	
	The System/solution should support automatic key management to ensure it can always respond to queries with DNSSEC-compliant responses by dynamic generation of new keys and automatically removing a key when it expires.	
Global Server Load Balancing feature for DC & NDC Application	DNS architecture should enable the DNS query load to be distributed across many locations for dynamic application delivery (User application requests and application services are distributed based on business policies, data center conditions, network conditions, and application performance)	
	Able to resolve DNS queries based on application-centric monitoring, persist user connections by querying Application Load Balancers across applications and all data centers and be automatically routed to the appropriate data center or server, based on application state, ensuring that users are directed back to the same site regardless of their entry point.	
	Native Support for SRV records in GSLB - DNS services capable of incorporating Service Provider protocols with NAPTR and SRV records abstracting intelligence for network optimization.	
	Able to support static and dynamic load-balancing algorithms such as Global availability, LDNS persistence, Application availability and Geography based load-balance.	
	Provides global high availability and reliability of applications across multiple sites and ensures application availability by tracking and managing interdependencies between applications.	
	Able to provide flexibility in having deterministic probes which communicate with each node to determine its availability, status, proximity, or responsiveness.	
	Able to perform intelligent probing of data center network resources to determine whether the resources are up or down. This allows to specify which device probe specific servers for health and performance data.	
	Able to provide manual GSLB configuration copy. This scalability feature for large configuration with rapid user changes can be saved manually.	
Anti-DDOS Solution Architecture and Features Requirements	The DDOS mitigation should have advanced detection mechanism which will detect the application or network performance, detect protocol anomaly, detect application anomaly based on particular DDOS attack as behaviour analysis and protect with dynamic filtering, IP address source tracking, creating dynamic signature and in-depth policy control.	

RESTRICTED

	Shall be IPv6 compliant and be deployed inline mode	
	Shall Detect and protect from unknown Network DDOS attacks/ Network behavioral based dos mitigation to detect and prevent zero-day DoS/DDoS flood attacks. The proposed solution must support at least 80M Syn Cookies.	
	Solution should support Network-wide protections:	
	Protection against flooding attacks, including: <ul style="list-style-type: none"> •ARP Flood •ICMP Flood •IGMP Flood •UDP Flood •IP Fragment Flood •LAND attack •TCP SYN Flood •Eavesdropping •Protocol abuse • TCP half Open protection 	
	— SYN protection—Protection against any type of SYN flood attack using SYN authentication mechanism.	
	The solution should support out-of-band DDOS Protection based on IPFIX/NetFlow data analysis, fast attack detection, and safe out-of-band mitigation.	
	Solution should Inspect all incoming client connections and server-to-client responses, and mitigate threats based on security and application parameters before forwarding them on to the server	
	Should support auto thresholding of DOS vectors	
	Connection Limiting: <ul style="list-style-type: none"> • Connection limit per source IP, dynamic backlisting per source IP violating the threshold. • Inbound and outbound threat protection 	
	The solution should support remotely triggered black hole filtering (RTBH) with IP shun category to stop attack traffic and blocks malicious L3–L7 attack sources by automatically broadcasts malicious IPs to upstream routers and enforce denylisting through routers, ensuring that only good traffic is routed to the data center network and applications.	
	The device should support Whitelisting and blacklisting IP addresses. Also, it should support dynamic blacklisting of offending sources	
	The Solution should be able to DNS security with built-in protocol validation in software to automatically drop high-volume UDP, DNS query, NXDOMAIN floods, and malformed packets and mitigate below DNS attacks: <ul style="list-style-type: none"> • Phantom Domain Attacks • NX Domain Attacks • Random Subdomain Attacks • Lock Up Domain Attacks • Amplification Attacks • DNS Tunneling Attacks • Malformed Packet Attacks 	

RESTRICTED

	<ul style="list-style-type: none"> • Cache Poisoning Attacks • DNS record type ACL* 	
	Solution should provide full SSL visibility at scale, as well as network-layer and session-layer DDoS mitigation.	
	The solution must be able to provide dynamic threat intelligence and service based on source reputation. The feed must be provided the following known attack sources(Spam sources/Windows exploit/Web attacks/Botnets/Scanners/Denial of service/Infected sources/Phishing/proxies/Tor proxies)	
	The system Shall have inbuilt reporting engine.	
	SIEM integration through Syslog messages with High speed logging to allows visibility into incident and status events, logging and reporting	
	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity:	
	- Ability to drop requests & response	
	- Block the TCP session, user, IP	
	The solution must be able to perform profiling of web applications in an environment where there is a mixture of good & bad traffic. The solution must be able to automatically differentiate good & bad traffic when learning the profile. Bad traffic shouldn't be learnt.	
Cloud Scrubbing Capability and requirement for Anti-DDoS	The proposed solution should support cloud based DDoS mitigation. This cloud based anti-DDoS support the integration with on-premise Anti-DDoS solution as a Hybrid DDoS Mitigation solution. This Cloud DDoS Mitigation solution can be on-board anytime if required in future.	
	The proposed solution should support Integration with technology OEM owned DDoS scrubbing center. The DDoS scrubbing center should have at least 13 Tbps mitigation capacity or higher.	
Dashboard	The solution must have an integrated dashboard containing various features of alert and report generation including CPU, Memory , Connections , Throughput , Pool, Node, also should have details visibility for Cloud Scrubbing solution traffic from Scrubbing center console.	
Configuration, Visibility & Reporting	The solution must provide automated, real-time event alert mechanism.	
	The Solution should provide a catalog of DoS and DDOS service templates to quickly configure and rapid roll out new network services. It also supports replicate existing service templates and modification.	
	The Solution must have dashboard to see L3-L4 Anti-DDoS Policy, device protection policy and visibility of traffic.	
ICSA Certification	The Proposed Solution should be ICSA certified. Bidder must submit the OEM's certificate.	
FIPS Compliance	The proposed solution should support FIPS 140 Level 2.	

RESTRICTED

ISO Certification	The OEM/Manufacturer should have ISO 9001, ISO 14001 and ISO 27001 Certification. Bidder must submit the OEM's ISO certificates.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

30. Application Delivery Controller (ADC), Web Application Firewall & API Security		
Items	Required Technical Specifications	Bidder's Response
Brand	Internationally reputed brand. To be mentioned by Bidder.	
Model	To be mentioned by the bidder (Preferably F5)	
Country of origin	As per tender specification, article 20	
Manufacturing Country	As per tender specification, article 20	
Solution Architecture Requirement	The proposed solution have to perform as a dedicated appliance-based Next Generation Web Application Firewall (WAF), Application Access Management, Load Balancer and Application Layer Encryption considering as Data Center Application Delivery Controller solution also run on the same hardware platform. Relevant solutions should be Scalable and on single OS and Hardware platform. The proposed hardware appliance management OS should be containerized platform based modern architecture and Multi-tenancy platform OS.	
	The solution must support both Forward Proxy and Reverse proxy mode as a full proxy (Forward Proxy & Reverse Proxy) architecture to control separate user sessions and separate application sessions on ingress and egress point for more control and complete visibility of security on layer 3 to Layer 7.	
	Proposed device must support multi-tenancy with partitions based on purpose-built isolation mechanism of the tenants at the device level. The proposed solution should support minimum 8 tenants / guests in isolated environments from day -1 and It can be upgrade up to 26 tenants in future without changing hardware platform.	
	The proposed Load Balancer license, WAF License and Access Management License should be perpetual and 64-bit software Architecture.	
Management System	The entire solution should support integration with central management system to centrally manage Load Balancer policies, Application access Management polices, WAF Policies, L7 DDoS Policies and BoT Policies for day to day operations from single console.	
	Management Port : 1x 1000BASE-T,1x USB 3.0,1x serial console	
	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot or on device packet captures on appliance config and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link.	
Appliance Resource	The appliance should have minimum 128 GB DDR memory or higher.	
	The appliance should have minimum one 1TB SSD drives or higher	

RESTRICTED

	The proposed system must have redundant power supply from Day 1.	
	The Proposed Hardware Appliance must be 1U rackmountable Appliance.	
	<p>The proposed solution should have minimum</p> <ul style="list-style-type: none"> • 8 x 25G/10G SFP28/SFP+ ports • 2 x 100G/40G QSFP+/QSFP28 ports from day 1. <p>Bidder has to propose 8 x 10 GE SR SFP+ module for each appliance and 2 x 40G QSFP SR Module for each appliance. All the SFP module should be same OEM original SFP.</p>	
	The proposed appliance should support 2.5M L7 request per second from day1 and it can be upgradeable up to 4.3 million on the same hardware platform in future.	
	The proposed appliance should support 95Gbps of L4 throughput & 60 Gbps of L7 Throughput from day 1 and it can be upgradeable up to 95GB Throughput for L7 within the same hardware platform in future.	
	The proposed appliance should support minimum 75 Million L4 concurrent connections from day 1 and it can be upgradeable to 100 Million within the same hardware platform in future.	
	The proposed appliance should support 18 million L4 HTTP request per second from day 1	
	The proposed appliance should support 35 Gbps of SSL based hardware offloading throughput from day1 and It can be upgradeable up to 50 Gbps on the same hardware platform in future.	
	The SSL encryption & decryption process must be hardware-based processor for acceleration.	
	The proposed appliance must support minimum 60K SSL TPS (2k SSL) from day 1 and It can be upgradeable up to 100K TPS on same hardware platform in future.	
	The proposed appliance must have minimum 35 Gbps Hardware-based compression throughput for HTTP traffic from day 1 and it can be upgradeable to 50 Gbps on the same hardware platform.	
	The appliance should have 80M SYN Cookies per second hardware DDoS protection for proposed appliance DDoS protection.	
	6vCPU Reserved for Control Plane OS and 12 vCPU's Available for Multi-Tenancy and Data-plane from Day 1. It can be upgradeable up to 26 vCPU's for Multi-Tenancy on the same hardware platform in future.	
	The Proposed solution should have multi tenancy capability within the same appliance, where tenancy consist with dedicated OS, vCPU, RAM and storage along with tenant wise administrative priviledge.	
	The proposed solution should allows for configuration of up to 2000 virtual route segment or VRF on proposed solution that support Layer 3 virtualization, traffic	

	segmentation, routing isolation for traffic security within the tenant.	
	The proposed solution must have multiple license provision option within One tenant and also all the licenses must be shareable within the all of the tenants on the same appliance.	
Load Balancing Feature	The solution must have application level load balancing including the ability to act as HTTP 2.0 Proxy.	
	The solution must have TLSv1.0, TLSv1.1 and TLSv1.2 and TLSv1.3 on both Client and Server side.	
	The solution must have full proxy architecture with HTTP Keep-Alive to allow the load balancer system to minimize the number of server-side TCP connections by making existing connections available for reuse by other clients for TCP optimization.	
	The solution must have server load balancing algorithms like (but not limited to) 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, Observed, Predictive, Least session, least connections, super http, least latency, weighted round robin and TCL based script for customized algorithm etc.	
	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers.	
	The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.	
	To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user.	
	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL persistency mirroring, HTTP Compression, caching etc. in active-passive mode. All the feature should be enabled in Full-Proxy Mode.	
Web Application Firewall Feature Requirements	The solution must be able to protect both HTTP Web Applications and SSL (HTTPS) web applications. It should have support for ECC keys along with RSA keys.	
	WAF must have capability to protect Credential Attacks Protects against attacks that can steal credentials from the user's browser through browser-based malware, from data in transit and/or from the server without installing any agent at client machine	

RESTRICTED

	<p>The WAF solution must support all major cipher suites like Camellia Ciphers Suites, SSLv3 and TLSv1.3 implementation for strong encryption. The WAF solution must support elliptic curve cryptography (ECC) acceleration in hardware.</p>	
	<p>The solutions should defend against the OWASP Top 10 Vulnerabilities and should able to edit/change the security policy on the fly during the real time attack on the particular network or particular application</p>	
	<p>Solution should have a layered Policy structure (Policy Inheritance-Parent/child policy) to establish uniformity in terms of web security posture for their backend web applications to identify policy differences instantly which will help admin to identify issues quickly in times of misconfiguration/ human error and also to make new policies quickly.</p>	
	<p>The solution must have Application layer DoS and DDOS attacks protection including nxdomain, stress-based DOS and Heavy URL attacks.</p>	
	<p>The solution must support custom security rules. Administrators should be able to define rules for the positive and negative security model and to create correlation rules with multiple criteria or capable with violation correlation engine. This should be possible without need to write any script/code.</p>	
	<p>The solution should support protection against common attacks such as SQL Injection, Cross-site Scripting, Cookie or Form Tempering etc.</p>	
	<p>The solution must support integration API based integration with industry leading Dynamic Analysis Security Testing (DAST) tools of IBM, HP, Rapid7 etc. to perform virtual patching for its protected web applications.</p>	
	<p>WAF should have capability of Proactive BOT Defense (both detection and Protection) mechanism beyond signatures and reputation to accurately detect malicious and benign bots using client behavioral analysis, server performance monitoring, and escalating. The BOT defense feature should have Predefined Bot Defense profile to enable quicker and easier BOT defense configuration.</p>	
	<p>Solution must have protection against Layer 7 Application DDOS type of attacks in full-Proxy Mode (Forward Proxy and Reverse Proxy) using machine learning mechanism form day 1.</p>	
	<p>The proposed solution should be equipped with pre-defined web server technologies/backend host based on which a customized Policy can be configured and hardened, for - AngularJS, Apache Tomcat, ASP.NET, CGI, Backbone.js, BEA Systems WebLogic Server, Elasticsearch, Front Page Servver Extension, Google Web Toolkit, GraphQL, IBM DB2, IIS, JSP, JSF, JBoss,</p>	

RESTRICTED

	Jenkins, JQuery, MongoDB, MySQL, Node.js, Oracle, PHP, Python, Sybase, WebDAV, XML, Oracle Application Server etc.	
	The proposed WAF solution should have dynamically updated threat intelligence to protect against coordinated and organized BOT attacks and threats from malicious source.	
	The solution should be able to encrypt the user credentials in real time i.e. when the user is typing the credentials for the web application in his/her browser for any web application that is behind the WAF. This feature should be agentless and should not require installation of any kind of software either on client end or on the application end.	
	The solution must have capability of blocking access to specific URL path based on client-source-IP.	
	The solution must have capability to restrict Restricting specific user (Administrators / web-admin / SQL admins) login from outside of network.	
	The solution should be able to perform validation on all types of input including URLs, forms, cookies, query strings, hidden fields and parameters, HTTP methods, XML elements and SOAP actions.	
	The solution profiling technology should be able to detect and protect against threats which are specific to the custom code of the web application. After the learning phase, the solution must be able to understand the structure of each protected URL and must be able to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.	
	The solution should allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	
	The solution must able to encrypt the user credentials of the protected applications in real time by encrypting the password without any agent either on the client side or on the server side. This feature could be activated at any time with additional license on the WAF when required.	
Customizable Authentication and Authorization Features	Solution must have specify different authorization policies for different parts of the websites, post authentication. Solution should support users access management with the same appliance.	
	Solution must have 500 concurrent user connectivity capacity from the day 1 and it can be scalable upto 20000 concurrent user connectivity within the same hardware platform if required future.	
	Solution must have access control to Portal access, Application tunnels, and network access through SSL VPN with AAA server authentication and high availability	

RESTRICTED

	and Step-up authentication, including multi-factor authentication (MFA) within the same appliance.	
	Solution must have Single Sign-On (SSO) with support for Kerberos, header-based authentication, credential caching, and SAML 2.0, SSL VPN remote access and L7 access control list (ACL) within the same appliance.	
	Solution must have API Authentication, Authorization along with support for inspection, rate limiting, behavioral analysis, anti-automation, detects application program interface (API) threats and API protocol security check to secure REST API, JSON, XML/SOAP and Gateway APIs within the same appliance.	
	Solution must have creation of customizable webtops for users login process. The webtop must provide a policy branch to which network access resource, portal access, Application tunnels, Remote Desktop etc., with integration of MFA, such as, SMS based OTP within the same appliance.	
API Security	The solution must have API inspection, rate limiting, behavioral analysis, anti-automation, detects application program interface (API) threats and API protocol security check to secure REST API, JSON, XML/SOAP and Gateway APIs.	
	WAF Should Support the API Security with Enforcement mode to ensure the API security including API Parameter, request header, API Payload security.	
	API endpoints, whether imported via the OpenAPI document import, discovered, or manually configured, so all HTTP requests with matching method and path are allowed, blocking illegitimate requests.	
Dashboard	The solution must have an integrated dashboard containing various features of alert and report generation including CPU, Memory , Connections , Throughput , Pool, Node,	
Configuration, Visibility & Reporting	The solution must provide automated, real-time event alert mechanism.	
	The Solution should provide a catalog of application service templates to quickly configure and rapid roll out new app services. It also supports replicate existing service templates and modification.	
	The Solution must have Single Pan dashboard to see WAF Policy, L7 DDoS Policy, BOT Protection attached to load balancing IP based on per application.	
	The solution should have Domain/URL based Policy Configuration to override the security policy enforcement Mode for Learning and Blocking Settings for a defined unique identifier of Server Hostname + URL from Single Window Configuration panel.	
PCI DSS Compliance and OWASP top	The proposed WAF should provide PCI DSS compliance and OWASP top 10 compliance dashboard	

10 Compliance dashboard		
ISO Certification	The OEM/Manufacturer should have ISO 9001, ISO 14001 and ISO 27001 Certification. Bidder must submit the OEM's ISO certificates.	
MAF and Manufacturer's part number	Bidder must submit the OEM's certificate. Bidder should submit BOQ of proposed device including the details part numbers and Manufacturer's Warranty part number.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	Training
Warranty	OEM must have local RMA depot in Bangladesh for faster delivery on faulty hardware / parts replacement issue to avoid business criticality on RMA replacement.	
	Manufacturer's warranty part number should be mentioned, minimum 03 (Three) years warranty for technical solution support with Patch & New Software Upgrade should be provided for the proposed solution. OEM should have local representative and depot in Bangladesh for RMA replacement within Next business day.	

Technical Specification of Storage		
31. Storage		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned by bidder. (Preferably Hitachi Vantara/NetApp)	
Model	To be mention by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Architecture	<ul style="list-style-type: none"> The proposed array must be a true All Flash Storage with Minimum Dual hot-swappable Active-Active controllers with NSPoF architecture & 99.999% availability guarantee from Day 1. The Proposed array should be non-disruptively scalable to at least 4 controllers or higher and should support End to End NVMe technology. Designed to take advantage of the Flash/SSD/NVMe for high performance, reliability, energy efficiency and consistent performance. The proposed array should be a unified storage supporting block, file services and VVOL natively or adding any additional or external device 	
Gartner Magic Quadrant	Bidder must be listed in leader quadrant of Gartner MQ report for All Flash storage for last 3 years. Bidder should propose their latest storage models and solutions in response to this RFP.	

RESTRICTED

Storage Processor and Cache	<ul style="list-style-type: none"> Proposed storage solution should have All Flash Storage Array having 2 x dual-socket Intel CPUs/ASIC Based minimum 24 core processor per controller or equivalent, with minimum 1024 GB data cache per Array from Day 1, upgradable up to 4096 GB of capacity for the array. 	
Front End Ports	The proposed storage array should be configured with at least 16 x 32Gbps FC ports and at least 8 x 10GbE ports to provide scalable and dedicated connectivity to hosts and for remote replication.	
Backend Connectivity	Offered Storage Should be configured with at-least 4 or more numbers of NVMe backend ports across Dual controllers to achieve minimum 300K IOPS with less then 1 MS response time.	
Capacity and Performance Requirement	<ul style="list-style-type: none"> The proposed array must be configured with 200 TB usable capacity after RAID 6 or dual parity (8K block size, 80% Read & 20% Write) or equivalent from Day 1, The proposed storage should support 3.84 TB SSD drive or less capacity and minimum 300K IOPS with less than 1 MS response time from Day 1. The proposed storage should come with its OEM make rack. Proposed storage solution must be scalable to minimum 10 PB RAW capacity with ability to increase capacity. 	
Data protection	Proposed storage should support global hot spare or hot spare for two disk failure and three disk failure simultaneously. The proposed storage should have No Single Point of Failure and support all hot swappable components. The Storage array should guarantee no data loss in the event of a power failure in the data center and a component failure in the storage.	
Power supply	Dual, Hot -plug Redundant power supplies	
Data Reduction for Space Efficiency	The proposed array should support enterprise class data services including - Thin Provisioning, Inline Compression & Deduplication, Replication, Snapshot (with ROW algorithm). Storage should allow enable/disable of data services per application storage groups (single or group of LUNs). Data reduction must be supported on block (FCP, iSCSI) and file (CIFS, NFS) data	
Data Encryption	The proposed array must support storage controller-based Data at Rest Encryption solution to encrypt data on all drives. If Controller base Encryption not supported, please proposed all SED drives with required license.	
Scalable File System	The proposed array must support traditional (user data) and transactional (VMware, Oracle) NAS use cases. Proposed storage solution must support creating multiple	

RESTRICTED

	NAS servers for tenant isolation with each file system scalable up to 16TB.	
Host Integration	The proposed bidder should include host based multipath management for 75 hosts from Day 1 to support end-to-end stack connectivity (if OS native multi path not supported by array)	
Dial Home Support	Proposed array should support dial home notification feature for proactive case logging. Dial home data should be accessible to IT team.	
Quality of Service	The proposed array should support QoS feature to limit the amount of IO (IOPS) or bandwidth (MB/s) a particular application can drive on the array.	
Storage Management Software	The proposed array should be supplied with native Storage management software with Web based GUI capable of generating customized reports, real time monitoring, historical performance data for analysis and trending, capacity utilization monitoring. Proposed management software should support management of multiple storage system from single console.	
Cloud Based Monitoring and Reporting	Proposed solution should also have cloud-based monitoring and management tool with support for 2 years of historical reporting. Software should support monitoring and reporting multiple storage system, VMware environment and SAN switches. Required on-prem software and hardware should include in the solution. Cloud based software should be accessible from any internet connected device with mobile application support for iOS and Android.	
Snapshot	Proposed storage solution should support snapshot creation using ROW algorithm. Storage arrays should have ability to use snapshot as writable volume. Proposed system should support snapshot scheduler. Proposed storage should allow snapshot replication with different retention for source and destination from Day 1.	
Application Aware Automation and Orchestration	Proposed storage solution should include software to automate and orchestrate application/databases data management - including but not limited to MSSQL, Oracle, Exchange etc - to create application/database consistent copy for multiple use cases including data repurposing, off-host backup, Test/Dev, Reporting etc.	
VMware Integration	Proposed storage solution should support VMware VAAI, SRM, VASA, VVOLs and VMware cloud foundation for multi-cloud data mobility. Detailed document to be provided for the same. Proposed storage should include software to create VM consistent point-in-time copies with support for granular data restoration.	
Security Compliance	<ul style="list-style-type: none"> Proposed storage must have USA DOD Approved Products List (APL), Controller Based Data at-rest Encryption (D@RE), HIPPA compliant, TLS 1.2 support, native SHA certificate support, IPV dual stack certified, FIPS 140-2 Level 1 certification, Common Criteria Certification international 	

RESTRICTED

	<p>standard (ISO/IEC 15408) for computer security certification, KMIP compliant, STIG CAT1 and CAT2 compliance</p> <ul style="list-style-type: none"> Proposed should have all the PCI-DSS compliant from Day 1. 	
Installation & Commissioning	Bidder should submit High-level, Low-level design documents from vendor.	
	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware / software required to make the network functional and shall provide respective documentation to IT Division.	
	Bidder should perform UAT and submit UAT signoff documents.	
	Bidder should submit project closure and operations.	
	Bidder should submit documents to perform daily operations.	
Form Factor	Bidder should mention	
Rated power	Bidder has to mention	
Support & Warranty	<ul style="list-style-type: none"> 3-years warranty including 24 x 7 x 365 days technical support and assistance by Manufacturer with 4 hours SLA for part replacement. OEM should have in-country product depot/warehouse. But in case OEM don't have a depot/warehouse all critical parts should be stored in the bidder location. OEM should have direct mail access support and toll-free contact number for customer to contact directly for any troubleshooting issue 	
OEM Certified Training	<ul style="list-style-type: none"> OEM Certified Training on Install configure and manage storage for 6 persons in two batch in OEM certified training institute by an OEM certified trainer. If training happens in abroad all expenses (airfare, travel local and abroad, accommodation, fooding and etc.) have to be borne by the bidder. 	

32. Back Up Storage Server

Features List	Feature Description	Bidder Response
Brand	To be mentioned by bidder. (Preferably Hitachi Vantara/NetApp)	
Model	Should be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	

RESTRICTED

Controller	Minimum Dual controller (Active-Active). Each controller CPU should be based on Intel processor minimum 10 core @ 1.5 GHz or higher	
Memory (Cache)	Minimum 32 GB system memory (per controller) total 64 GB in storage system	
	Must provide 50 TB usable capacity under RAID 6 from Day 1	
	Must provide adequate spare drives	
	The storage should grow minimum of 2 PB of raw capacity	
	The system should support NLSAS/SAS/SSD and SED drives	
	Offered system should be able to provide up to 150K IOPs performance from Day 1	
	System should be able to provide up to 250 MB/sec bandwidth for write operation	
	<ul style="list-style-type: none"> Offered system should be able to provide up to 900 MB/sec bandwidth for read operation Must support performance at scale with 12G SAS backend. Must come with OEM manufactured rack. 	
Storage expansion	The array must be scalable at least 140+ drives without controller upgrade/ replacement/ adding or external storage virtualization	
Front/Back End Ports	<ul style="list-style-type: none"> Each controller must be configured with 4 x 16G FC interfaces populated with the transceivers. 	
	<ul style="list-style-type: none"> The system should have the capability to run simultaneous multiprotocol. 	
	<ul style="list-style-type: none"> Must have 12Gb SAS backend 	
Raid support	RAID 0, 1, 5, 6, 10, 50 and/or dynamic/advanced RAID levels that reduces rebuild times when drive failures occur; any combination of RAID levels can exist in single array	
Auto Tiering	Good to have support for 3 Level Tiering for improved performance and efficiency	
Thin Provisioning	Should be active by default on all volumes, operates at full performance across all features	
Snapshot	The storage system should support snapshot, minimum 1000 per array from Day 1	
Volume copy	The storage system must support volume copy for seamlessly clone volumes from Day 1	
NAS Functionality	Provide system must come with NAS functionality with minimum 4x10gbps SFP+ SR. from Day 1.	
Replication	The system should support IP or FC remote replication. The system should have the capability to replicate data to any global location that includes mirroring thin provisioned pools	

RESTRICTED

	<p>Target/source relationships may be one-to-many or many-to-one</p> <p>All the above features should be present from Day 1 with required license.</p>	
Security	<p>Self-encrypting drives (SEDs) in SSD or HDD formats</p> <p>Full Disk Encryption (FCE) based on AES-256</p> <p>Drives certified to FIPS 140-2 Level 2</p> <p>Must offer controller based Internal/External Key Management system from day 1</p>	
Host OS Support	<p>Windows 2019, 2016 and 2012 R2</p> <p>RHEL 6.9 and 7.4</p> <p>SLES 12.3</p> <p>VMware 6.7, 6.5 and 6.0</p>	
Power supply	Dual, Hot -plug Redundant power supplies	
Management	Proposed system must provide integrated HTML5 web-based management interface for anywhere, anytime control. It should also support CLI and REST API.	
Form Factor	Bidder should mention	
Spare Parts	<p>Supplier has to sign a SoR agreement for Hardware & Software where all license scenarios should be captured.</p> <p>Supplier has to provide a list mentioning individual hardware/spare parts/ license item and price, which will be used to expand the infrastructure.</p>	
Installation & Commissioning	<p>Bidder should submit High-level, Low-level design documents.</p> <p>Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware / software required to make the network functional and shall provide respective documentation to IT Division.</p> <p>Bidder should perform UAT and submit UAT signoff documents.</p> <p>Bidder should submit project closure and operations.</p> <p>Bidder should submit documents to perform daily operations.</p>	
Rated power	Bidder has to mention	
Support & Warranty	<ul style="list-style-type: none"> • 3-years warranty including 24 x 7 x 365 days technical support and assistance by Manufacturer with 4 hours SLA for part replacement. • OEM should have in-country product depot/warehouse or OEM / Supplier should have in-country arrangement for Critical Spare part availability. • OEM should have direct mail access support and toll-free contact number for customer to contact directly for any troubleshooting issue 	
OEM Certified Training	<ul style="list-style-type: none"> • OEM Certified Training on Install configure and manage backup storage for 4 persons in two batch in OEM certified training institute by an OEM certified 	

	trainer. If training happens in abroad all expenses (airfare, travel local and abroad, accommodation, fooding and etc.) have to be borne by the bidder.	
--	---	--

Technical Specification of Security Solution

33. WEB Security Appliance (WSA)		
Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Part No	Bidder should submit the required feature & performance compliance document for the proposed solution.	
Platform Requirement	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance for at least 600 users. All the functionalities should be in a single appliance from the day 1.	
	The solution should provide content filtering capabilities for laptop users who access the internet through data cards or public internet. Same content filtering policies should be applied for mobile laptop users when laptop is outside on public network. Solution cited should have provision for cloud/in-house policy sync server through which remote filtering clients should update the policies automatically; for any change in policy on the mail console same should be replicated for remote users automatically. License for 200 laptop users should be provided in solution to start with.	
	The solution should support policy enforcement for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints. And this solution should be on premises or Cloud based, but not with the help of VPN or complete traffic redirect to corporate network.	
	Solution shall support credential caching (for transparent and explicit proxy) to reduce load on domain controllers.	
	Should support active/active High Availability mode	
	The solution should be hardware based	

RESTRICTED

Hardware Architecture	The solution should have minimum 6x1G Copper Interface	
	The solution should have minimum 32 GB Memory	
	The solution should have redundant power supply from day 1	
	The solution should have minimum 1 TB storage	
Quantity	04	
Proxy Feature	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.	
	The solution should also support transparent mode deployment using WCCP v2 dual IP proxy configuration and L4 switches/PBR (Policy-based Routing)	
	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis	
	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's. The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.	
	Should have the ability to proxy, monitor, and manage IPv6 traffic.	
	Solution must have Time based quota policies which can applied to users/ groups/Ous etc.	
	The solution should allow to schedule centralized configuration push to Proxies.	
	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.	
Security Features	Should have min 20+ million websites in its URL filtering database and should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls.	
	The solution should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page and creation of custom URL categories for allowing/blocking specific destinations as required by the Organization. The solution should have facility for End User to report Mis-categorisation in URL Category.	
	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different	

RESTRICTED

	domains to assign a web based score to determine the likelihood that it contains url-based malware.	
	The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.	
	When the website is blocked due to suspected malware or URL- Filters it should allow the end user to report that the webpage has been wrongly misclassified.	
	The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.	
	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.	
	The proxy should support the functionality to configure URL feeds as custom categories	
	The proxy should support the functionality to exempt URLs/lps downloaded from the feed server	
	The Proxy should support Multi category URLs filtering	
	The solution should support HTTPS decryption from day one should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.	
	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80.	
	Should inspect the sensitive content through pre-defined templates, textual content inside image, cumulative content control and inspection through web channel to prevent the content from being sent over outbound web channel.	
	The appliance should support at least 2 industry known Anti Malware/Anti Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Key loggers and as defined by the organizations policy. Please mention the antimalware engine.	
	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.	
	The solution should support signature based application control.	
	Solution should support filtering adult content from web searches & websites on search engines like Google.	

RESTRICTED

	Should simplify design and implementation of policy to ensure user compliance	
	Should have ability to block anonymizer sites or proxy avoidance tools.	
	The Proxy should support ability to filter YouTube Video categorization	
	The proxy should support ICAP/ICAPs integration for external DLP	
	The solution shall provide option to choose Multiple Antivirus engines	
	The proxy should support VDI users identification	
	The proxy should support TLS 1.3	
	The proxy should support HTTP 2.0	
	The Solution should allow admin to choose source IP as IP spoofing feature	
	The solution should support integration with Private File reputation and sandbox integration	
	The proxy should offer ability to block files based on the file name and file types	
	The proxy should offer ability to Add/Remove/Edit HTTP custom or default headers	
	The proxy should offer ability to consume Authention header from downstream proxy	
	The proxy should offer Office 365 or Cloud Application restriction based on the user/group header/custom headers.	
	The proxy should offer ability to anonyms User information in the logs	
	The proxy should allow exempting traffic from decryption and further scanning	
	The proxy should offer ability to block file upload and download based on the file size	
	The solution should support SOCKS4 and SOCKS5	
	Solution should provide different action based on categories, protocols, file type, UDL, keyword, regular expression, User, Group, OU, Domain, IP address, etc.	
	Offered solution should have real time reputation service for both IP's and URL's	
	Solution must be capable of inspecting SSL traffic within the same appliance with no additional hardware required.	
	Offered solution must support the real-time graphical and chart-based dashboard for the summary of WEB filtering activities.	
	The frequency of updates to the master threat and URL databases should be configurable.	
	Solution must not be just signature based security but also should have other predictive engines to provide real time checks	
	The solution must be able to detect and prevent unknown exploits using behavioral technology	

RESTRICTED

	The solution must be able to detect and block suspicious user agents	
LDAP Support	The solution must seamlessly integrate with LDAP, Active Directory and Radius server for user authentication and authorization.	
Administration, Management and Reporting	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH/SSL for troubleshooting purposes	
	The appliance should be manageable via command line using SSH and must have serial console access on appliance for emergency scenarios	
	The appliance based Solution should be provided with hardened Operating System. No need of separate OS/database for management and reporting	
	Solution to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it. Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files. Solution should support to schedule reports to run on a daily, weekly, or monthly basis.	
	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.	
	The solution should support REST API for reporting and tracking.	
	The solution should support REST API for configuration.	
	The appliance should be manageable via centralized configuration manager	
	The solution should support centralized reporting and tracking feature.	
	The proxy should support automatic config backup	
	The proxy should allow to send logs to external server using Syslog, FTP and SCP to external SIEM/Logging server	
	The solution should support centralized software upgrade	
	The proxy should support 2FA for administrators for secure login to Proxies	
	Solution should have drill down reporting interface	
	System shall have method of notifying administrator of issues with proxy.	
	The appliance should be manageable via command line using SSH	
	For emergency, the appliance should have serial console access	
	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it	
Solution should support to schedule reports to run on a daily, weekly, or monthly basis.		

RESTRICTED

	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.	
	The appliance should provide seamless version upgrades and updates.	
	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

34. Network Access Control		
Feature List	Feature Description	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Part No	Bidder should submit BOQ of proposed device including the details part numbers. Bidder should submit the required feature & performance compliance document for the proposed solution.	
Network Access Control & Authentication Specification:	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform.	
	It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise.	
	Provides complete guest lifecycle management by empowering sponsors to on-board guests	
	The propose solution should have 1 unit of VM based Network Access Control & Authentication system with 1000 endpoints in the network. 1 unit device administration license from day one and 5000 growth plan for next 3 years.	

RESTRICTED

	Delivers customizable self-service portals as well as the ability to host custom web pages to ease device and guest on-boarding, automate endpoint secure access and service provisioning, and enhance the overall end-user experience inside business-defined workflows.	
	Offers comprehensive visibility of the network by automatically discovering, classifying, and controlling endpoints connected to the network to enable the appropriate services per endpoint	
	Addresses vulnerabilities on user machines through periodic evaluation and remediation to help proactively mitigate network threats such as viruses, worms, and spyware	
	Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention	
	Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations	
	Allows you to get finer granularity while identifying devices on your network with Active Endpoint Scanning	
	Augments network-based profiling by targeting specific endpoints (based on policy) for specific attribute device scans, resulting in higher accuracy and comprehensive visibility of what is on your network	
	Manages endpoint access to the network with the Endpoint Protection Service, which enables administrators to specify an endpoint and select an action - for example, move to a new VLAN, return to the original VLAN, or isolate the endpoint from the network entirely - all in a simple interface	
	Utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).	
	Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).	
	Offers a rules-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use	
	Provides a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging.	
	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.	

RESTRICTED

	<p>It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.</p>	
	<p>The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.</p>	
	<p>Solution should allow end users to interact with a self-service portal for device on-boarding, providing a registration vehicle for all types of devices as well as automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms.</p>	
	<p>Should support full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise.</p>	
	<p>Verifies endpoint posture assessment for PCs connecting to the network. Works via either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming to a company's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc), and applications. Solution should support auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies.</p>	
	<p>Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.</p>	
	<p>Enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, greatly simplifying administration by providing consistency in managing all these services.</p>	
	<p>Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.</p>	
	<p>Should be available as a physical or virtual appliance.</p>	
	<p>Should support consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed</p>	

RESTRICTED

	Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)	
	Solution should have capability to determine whether users are accessing the network on an authorized, policy-compliant device.	
	Solution should have capability to establish user identity, location, and access history, which can be used for compliance and reporting.	
	Solution should have capability to assign services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).	
	Solution should have capability to grant authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.	
	Solution should support Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance	
	Solution should have capability which allows users to add a device on a portal (My Devices Portal), where the device goes through a registration process for network access. Should allow users to mark as lost any device that you have registered in the network, and blacklist the device on the network, which prevents others from unauthorized network access when using the blacklisted device. Should have capability to reinstate a blacklisted device to its previous status in the My Devices Portal, and regain network access without having to register the device again in the My Devices Portal. Should also support removing any device in the enterprise network temporarily, then register the device for network access again later.	
	The portal used for Device registration (MY device Portal) should be customizable, allowing to customize portal theme by changing text, banners, background color, and images	
	Should provide a Registered Endpoints Report which provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time. The report should provide the following details	
	•Logged in Date and Time	
	•Portal User (who registered the device)	
	•MAC Address	
	•Identity Group	
	•Endpoint Policy	
	•Static Assignment	
	•Static Group Assignment	
	•Endpoint Policy ID	
	•NMAP Subnet Scan ID	
	•Device Registration Status	

RESTRICTED

Solution should have capability to look at various elements when classifying the type of login session through which users access the internal network, including the following:	
zenprise, Inc.	
•Client machine browser type and version	
•Group to which the user belongs	
•Condition evaluation results (based on applied dictionary attributes)	
Solution should classify a client machine, and should support client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispysware vendor support, and correct agent customization packages and profiles, if necessary	
Solution should support automatic provisioning of NAC agents	
Solution should support periodic reassessment for clients that are already successfully postured for compliance.	
Solution should support the following endpoint checks for compliance for windows endpoints:	
Check operating system/service packs/hotfixes	
Check process, registry, file & application	
check for Antivirus installation/Version/ Antivirus Definition Date	
check for Antispysware installation/Version/ Antispysware Definition Date	
Check for windows update running & configuration	
Solution should support following remediation options for windows endpoints:	
File remediation to allow clients download the required file version for compliance	
link remediation to allow clients to click a URL to access a remediation page or resource	
Antivirus remediation to update clients with up-to-date file definitions for compliance after remediation.	
Antispysware remediation to update clients with up-to-date file definitions for compliance after remediation.	
Launch program remediation for NAC Agent to remediate clients by launching one or more applications for compliance.	
Windows update remediation to ensure Automatic Updates configuration is turned on Windows clients per security policy	
Solution should integrate with the following MDM vendors	
Airwatch, Inc.	
Good Technology	
MobileIron, Inc.	
Zenprise, Inc.	
SAP Afaria	

RESTRICTED

	Fiberlink MaaS	
	Solution should support configuring MDM policy based on the following attributes	
	Device Register Status, Device Compliant Status, Disk Encryption Status, Pin Lock Status, Jail Broken Status, Serial Number, Manufacturer, IMEI, Os Version & phone number	
	Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.	
	Should support native supplicant profiles to enable users to bring their own devices into the network. When the user logs in, based on the profile that you associate with that user's authorization requirements, solution should provide the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. This should be supported over Microsoft windows, Apple Mac and iOS and Android devices.	
	Should support an endpoint identity group which is used to group all the identified endpoints on your network according to their profiles. Solution should create the following four identity groups in the system: Registered Devices, Blacklist, Profiled, and Unknown.	
	When endpoints are discovered on the network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.	
	Should support using a simple filter that you can use to filter endpoints. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created in the Endpoints page.	
	Should support an advanced filter that you can preset for use later and retrieve, along with the filtering results, The advanced filter filters endpoints based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.	
	Should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.	
	Support for importing endpoints from LDAP server. Should allow to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. Should support an LDAP server to import endpoints and the associated profiles, by using either the default port 389, or securely over SSL, by using the default port 636.	
	Should support multiple Admin Group Roles and responsibilities like HelpDesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin and System Admin	

RESTRICTED

	<p>Should support Role-based access policies which are access control policies which allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user.</p>	
	<p>Should support Identity source sequences which defines the order in which the solution will look for user credentials in the different databases. Solution should support the following databases:</p>	
	<ul style="list-style-type: none"> •Internal Users 	
	<ul style="list-style-type: none"> •Internal Endpoints 	
	<ul style="list-style-type: none"> •Active Directory 	
	<ul style="list-style-type: none"> •LDAP 	
	<ul style="list-style-type: none"> •RSA 	
	<ul style="list-style-type: none"> •RADIUS Token Servers 	
	<ul style="list-style-type: none"> •Certificate Authentication Profiles 	
	<p>Should Support the following Authentication Protocols</p>	
	<ul style="list-style-type: none"> •Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) and Protected Extensible Authentication Protocol (PEAP)—support for user and machine authentication and change password against Active Directory using EAP-FAST and PEAP with an inner method of Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) and Extensible Authentication Protocol-Generic Token Card (EAP-GTC). 	
	<ul style="list-style-type: none"> •Password Authentication Protocol (PAP)—support for authenticating against Active Directory using PAP and also allows you to change Active Directory user passwords. 	
	<ul style="list-style-type: none"> •Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)—support for user and machine authentication against Active Directory using MS-CHAPv1. 	
	<ul style="list-style-type: none"> •MS-CHAPv2—support for user and machine authentication against Active Directory using EAP-MSCHAPv2. 	
	<ul style="list-style-type: none"> •EAP-GTC—support for user and machine authentication against Active Directory using EAP-GTC. 	
	<ul style="list-style-type: none"> •Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)—Should use the certificate retrieval option to support user and machine authentication against Active Directory using EAP-TLS. 	
	<ul style="list-style-type: none"> •Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)—support for user and machine authentication against Active Directory using PEAP-TLS. 	
	<ul style="list-style-type: none"> •LEAP—support for user authentication against Active Directory using LEAP. <p>Must be able to differentiate policy based on device type + authentication</p>	

RESTRICTED

Should have Ability to authenticate at least one phone and multiple users on the same	
switch port without interrupting service	
Solution should support MAB and can further utilize identity of the endpoint to apply the proper rules for access. Mac Address Bypass is typically used for devices which do not support 802.1x	
Solution must support Non 802.1x technology on assigned ports and 802.1x technology on open use ports	
Solution should provide support policy enforcement through VPN gateways	
Solution must allow users access to the network in a worst case scenario in case of AAA server outages or any other reasons like WAN failure.	
Should support authenticating Machines and users connected to the same port on the switch in a single authentication flow	
Should support authenticating IP phones and users connected behind IP phones on the same physical port.	
Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors:	
* Profiling using MAC OUIs	
* Profiling using DHCP information	
* Profiling using RADIUS information	
* Profiling using HTTP information	
* Profiling using DNS information	
* Profiling using NetFlow information	
* Profiling using SPAN/Mirrored traffic	
Should be able to classify endpoints based on information like DHCP, CDP, and LLDP attributes using IOS sensor capabilities enabled on switches	
Should support Microsoft Windows Active Directory.	
Solution should support troubleshooting authentication issues by triggering session authentication to follow up with an attempt to authenticate again.	
Should support session termination with port shutdown option to block an infected host that sends a lot of traffic over the network.	
Should support the functionality to force endpoint to reacquire IP address that do not support a supplicant or client to generate a DHCP request after a vlan change.	
Troubleshooting & Monitoring Tools	
Should support evaluation of the configuration of the device with the standard configuration.	
Should support TCP dump utility & also support saving a TCP dump file.	

RESTRICTED

	Solution should support schedule reports to run and re-run at specific time or time intervals & send and receive email notifications once the reports are generated.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Subscription Period	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

35. Deep Discovery Inspection		
Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by the bidder. (Preferably Trend Micro)	
Model	To be mentioned by bidder	
Country Of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Type	On premises	
Solution functionality and supported features	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections. The solution should support minimum 95+ protocol.	
	The proposed solution should support the native CEF,LEEF format for SIEM log integration	
	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects & share the activity & detection log in central XDR datalake in cloud.	
	Proposed Anti-APT solution should perform advanced network detection and analysis of the enterprise's internal network	
	Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection	
	Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.	
	Solution should provide risk based alerts or logs to help prioritize remediation effort	
	Solution should be deployed on premise along with on premise sandboxing capability with customised virtual machine for sandboxing.	
	The proposed solution should be able to store Real payload of the detected threats	

RESTRICTED

The proposed solution should be able to store packet captures (PCAP) of all Malicious communications detected by sandbox	
The proposed solution should use OS Sandboxes for detecting zeroday malwares, This should not be a CPU or chip based function which is not field upgradable or customizable.	
Solution should have ability to detect/interrupt malicious communication	
Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth	
The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.	
Solution should be able to integrate with its own threat intelligence portal for further investigation, understanding and remediation an attack.	
Solution deployment should cause limited or no interruption to the current network environment.	
The proposed solution should able to work with the existing technologies for advance threat protection through web protocol	
The proposed solution should have the ability to support out-of-band detection	
The proposed solution should be able to detect (lateral moments) movement of the attacker without the need of installing agents on endpoint/server machines	
The proposed solution should not have any port based limitation and should support all ports.	
The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.	
The proposed solution should support minimum 4 Gbps traffic per second	
The Proposed solution should able to support minimum 4X SFP+ with short range module	
The Proposed solution should be able to support minimum 4x10/100/1000 RJ45 port.	
The Proposed solution should have Hot Swappable Power Supply	
The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	
The Proposed solution should be able to detect communications to known command and control centers	
The proposed solution should be able to detect reputation of url being accessed	
The proposed solution should be able to identify and help to understand the severity and stage of each attack	

RESTRICTED

	The proposed solution should have built in capabilities to add exceptions for detections	
	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list	
	The proposed solution should support Multiple protocols for inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	
	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	
	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.	
	The Proposed solution must provide a web service interface/API for customer to customize their own system integration	
	The Proposed solution must have capabilities to correlate the detections on the device itself.	
	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.	
Manufacturer's Authorization letter, Warranty and support	Bidder must be submitted Manufacturer Authorization form (MAF)	
	Bidder should submit BOQ of proposed Solution including the details' part numbers	
	Bidder must quote for necessary Licenses for 03 years including Technical Assistance Center support, software updates and subscription update support.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate required policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to Bangladesh Navy Authority.	

36. Network Detection and Response (NDR)		
Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder	
Model	To be mentioned by the bidder	
Environmental	Maintain International Quality Environmental Safety Standard	
Architecture	The solution should provide contextual network-wide visibility with an agentless approach across the entire network with knowledge of who is on the network and what they are doing. It should also help organizations to implement smarter segmentation customized to the business logic. It should provide actionable intelligence enriched with context such as user, device, location, time-stamp, application.	
	The solution should be able to use the existing network environment as a sensor grid to analyse traffic flow across the organization in a non-disruptive manner and utilizing the investment in the network and security solutions.	
	The solution should provide a full-featured Network threat analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.	
	Unsupervised and supervised machine learning alongwith probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.	
	The solution should be able to get threat intelligence from research team to make detections of malware activity with higher accuracy and efficacy including Botnets, C&C servers, Bogons, Tor Entry/Exit Nodes, Connections to bad reputation Nations and Dark IPs..	
	The solution should be a dedicated behaviour analytics solution delivering advanced Network Detection & Response	

RESTRICTED

	(NDR) use cases and not a subset capability of SIEM or PCAP solution.	
Functional Capabilities	The solution deployment must be capable of consuming flow based for telemetry across the network to achieve Network Detection & Response (NDR) outcomes.	
	The solution must be able to consume flow information from the network in the form of Netflow V5, Netflow V9, IPFIX, sFlow, Jflow, cFlowd, NSEL to perform behavioural analysis.	
	The system should be able to monitor flow data between various VLANS, including virtualized networks	
	The solution should detect common anomalous events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, peer-to-peer, etc.	
	The solution should be capable of detecting non-standard applications on known ports, traffic using incorrect ports/protocols, the use of forbidden application protocols etc.	
	The solution should be able to track device activities across the data center, remote network branches and the cloud. It should be able to report usage behavior across the entire network.	
	The solutions should provide the capability of behavioural analysis on a dynamic custom user-defined relationship between groups of network assets based on certain parameters like services, protocols and events.	
	The solution should be able to collect security and network information of servers and clients without the usage of agents.	
	The solution should be able to investigate on-demand the cryptographic parameters for sessions between a server and its clients i.e. Number of encrypted connections made to servers that store critical data, TLS version, Cipher suite being used, Data volume and Key length to quickly determine vulnerable and out of policy TLS sessions.	
	The solution should support the enrichment of a flow to provide information about source/destination - MAC/IP/Port numbers and country, application name, Bytes, Packets, TLS versions Client Side, TLS version and cipher in use from server side, Username, NAT device, etc. are available.	
	The solution should have the ability to state fully reassemble unidirectional flows into bi-directional conversations; handling deduplication of data and asymmetry and eliminate redudant telemetry to improve system performance.	
	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall/endpoints/NAT gateway that are associated with a single conversation and present them as a single bi-directional flow record including traffic traversing NAT devices.	

RESTRICTED

	The solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.	
	The solution should have capability to assign risk and credibility rating to alerts and hosts and present critical high fidelity alerts prioritized based on threat severity with contextual information on the dashboard.	
	The solution should be capable of detecting data exfiltration/hoarding categories not as a general anomaly in traffic.	
	The system should detect data exfiltration and unusual internal data transfers.	
	The system should have the capability to historically track the dates first/last seen, and summary of malicious activity.	
	The solution should provide compliance use cases to identify usage of insecure, legacy and deprecated encryption algorithms being used by servers on the network.	
	The solution should be able to detect insider threats and policy violations.	
	The dashboard of the solution should have the facility to be configured according to different roles.	
	The solution should support the capability of application profiling in the system and should also support defining custom applications present or acquired by the customer.	
	The tool should have capability for interactive event identification and creating business logic and policies for threat detection.	
	The solution should provide the capability to define custom policies to evaluate flow attributes such as byte ratios, services, process, name and more.	
	The solution should be capable of detecting and investigating emerging cyber threats that have evaded network border and endpoint defenses.	
Integrations	The behaviour analytics solution should be a dedicated solution supporting out of box machine learning algorithms and not a subset capability of SIEM or Forensic analysis.	
	The solution should be able to integrate with various SIEMs and SOARs available in the market for response actions.	
	The solution should Integrate with Identity management or other equivalent solutions to provide user Identity information in addition to IP address information throughout the system. It should allow creation of user groups based on Identity & provide mapping of User Name to IP address on a device.	
	The solution should integrate with a Network Access Control (NAC) solution to alert the admin, provide mitigation actions like quarantine / block / apply custom policies both automatically on the endpoint to block further spread of the malware/worm across the network without affecting legitimate traffic on the network.	

RESTRICTED

	The solution must support remote authentication for user access via TACACS+ and RADIUS.	
	The system should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues.	
Sizing and Scalability	The system should be a rack mountable hardware appliance based	
	Scalability of the solution should be such as to cover the entire enterprise network with 5,000 FPS from day 1 and ability to ingest up to 3,000,000 FPS with up to 200,000 FPS per appliance.	
	The solution should provide the capability to respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls.	
	The proposed solution should have Separate management appliance and Flow Collector Appliance	
	The management console should have 2x 28 Core CPU with 512 GB Memory	
	The solution should provide the capability to respond quickly and effectively with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls.	
	The solution should support up to 5,000 FPS on day 1 with possible expansion as required.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Support	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

37. Anti APT Solution (Sandbox)		
Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by the bidder. (Preferably Checkpoint/Cisco)	
Model	To be mentioned by the bidder.	
Type	Purpose built / Dedicated Hardware Appliance	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Form Factor	To be mentioned by the bidder.	
Anti-APT Hardware Performance	Solution must be dedicated hardware based appliance,	
	Solution must support either distributed or Inline deployment mode.	
	System throughput minimum 1 Gbps from day 1.	
	Solution must have 5 or higher Virtual Machine from day 1	
	Proposed appliance must have 16 GB	
	Proposed solution must NOT have any file size limit locally.	
	Proposed solution must be capable to sanitize minimum 30,000 files per day. Note: To comply this clause, vendor will offer multiple box with stack(if needed).	
Threat Prevention Solution Overview	Proposed solution must provide the ability to Protect against zero-day & unknown malware attacks before static signature protections have been created.	
	Proposed solution must provide zero-day phishing websites protection.	
	Proposed solution must provide dynamic security components.	
	Proposed solution must provide IoC feeds should support a significantly greater number of observables for URLs, Domains, IP addresses, and Hashes.	
	Support secure ICAP communication over TLS.	
Deployment Topologies	Proposed solution should be part of a complete multi-layered threat prevention architecture (with IPS, AV, AS, URLF, APP FW...etc.).	
	Proposed solution should support Network based Threat emulation.	
	Proposed solution should support Host based Threat emulation.	
	Proposed solution should provide both onsite and cloud based implementations.	
	Proposed solution should support 3rd party integration (public API).	
	Proposed solution should support deployment in inline mode.	

RESTRICTED

	Proposed solution should support deployment in MTA (Mail Transfer Agent) mode, inspect TLS & SSL.	
	Proposed solution should support deployment in TAP/SPAN port mode.	
	Proposed solution should not require separate infrastructure for email protection & web protection.	
	Device must support cluster installation in different GEO location (DC-DC/DR/NDC/RDC)	
File types supported by Anti-APT solution	Proposed Anti-APT solution must support following file types or more:	
	PE files (EXE, DLL, and others)	
	MS Office (all office extensions)	
	PDF, Flash, Java applets (JAR and CLASS)	
	Analysis of links within email messages	
	Support Compressed file type, like: ZIP, RAR, 7Z and similar.	
	Support for new Archive Formats - WIM, CHM, CramFS, DMG, EXT, FAT, GPT, HFS, IHEX, MBR, MSI, NSIS, NTFS, QCOW2, RPM, SquashFS, UDF, EFI, VDI, VHD, VMDK, LZH, ARJ, CPIO, AR.	
	A new log generates for every extracted file from the archive with its emulation results. This log contains the name of the archive file. Logs correlate easily between the archive file and those of the files it contains.	
Unknown Threat Extraction Features	Proposed solution must have Automatic Engine Updates	
	Proposed solution should have Enhanced Security and Productivity for the Different Modes of deployment.	
	Proposed solution must be capable to Prevent many more malicious files and content within the emulation window.	
	Solution must support Threat Extraction on ICAP server mode, in addition to Threat Emulation and Anti-Virus.	
Threat Extraction for web-downloaded documents	Proposed solution should be simple to use, easily enabled for an existing NGFW and does not require any changes in the network.	
	Capable to extends Threat Extraction, File Sanitization capabilities, to web-downloaded documents. Supported file types: Microsoft Word, Excel, PowerPoint and PDF formats.	
	Threat Extraction prevents zero-day and known attacks by proactively removing active malware, embedded content and other potentially-malicious parts from a file. Promptly delivers sanitized content to users, maintaining business flow	
	Allows access to the original file, if it is determined to be safe	
Threat Extraction (File Scrubbing/Flattening)	The solution should Eliminate threats and remove exploitable content, including active content and embedded objects	

	The solution should be able to Reconstruct files with known safe elements	
	The solution should Provide ability to convert reconstructed files to PDF format	
	The solution should Maintain flexibility with options to maintain the original file format and specify the type of content to be removed	
	The solution should Provide Automatic Threat Extraction	
Secure and Archieve File Protection	Proposed solution must have following file sanitization features from day 1:	
	Capable to inspect and remove malware from Password protected files/archives.	
	Capable to inspect and remove malware from Archived (compressed) files.	
Threat Prevention Updates	Vendor must provide the details of its threat prevention update mechanism and its ability to handle zero day attacks across all next generation threat prevention applications including IPS, Application Control, URL filtering, Anti-Bot and Anti-Virus...etc.	
	Vendor must provide details on the re-categorization of URL, under the circumstances that a website has been comprised and possibly distributing malware	
	Vendor should have the capability to provide incident handling.	
Advanced Threat Prevention	Proposed Anti-APT solution must have following Threat Prevention features from day 1:	
	– Advanced forensics details for Threat Prevention logs	
	– Ability to import Cyber Intelligence Feeds to the Security Gateway using custom CSV and Structured Threat Information Expression (STIX)	
	– FTP protocol inspection with Anti-Virus and Sandbox Threat Emulation	
	– Consolidated Threat Prevention dashboard provides full threat visibility across networks, mobile devices and endpoints	
	– Automatic updates to Threat Extraction Engine.	
	– Dynamic, Domain and Updatable Objects in Threat Prevention and HTTPS Inspection policies.	
	– Anti-Virus now uses SHA-1 and SHA-256 threat indications to block files based on their hashes.	
	– Anti-Virus and Sandbox Threat Emulation now use the newly introduced SSH inspection feature to inspect files transferred over the SCP and SFTP protocols.	
	– Improved support for SMBv3 inspection (3.0, 3.0.2, 3.1.1),	
– Manage your custom intelligence feeds through SmartConsole. Add, delete or modify IoC feeds fetched by the Firewall as well as import files in a CSV or STIX 1.x formats		

RESTRICTED

	<ul style="list-style-type: none"> – Threat Extraction is now supported on ICAP server mode, in addition to Threat Emulation and Anti-Virus – Improved use of IoCs for indicators based on source IPv4 and IPv6 addresses 	
Anti-Evasion Technology	The solution should have anti-evasion capabilities detecting sandbox execution.	
	Solution should be resilient to cases where the shell-code or malware would not execute if they detect the existence of virtual environment. (proprietary hypervisor).	
Time delays for File / Content Sanitization	Solution should be resilient to delays implemented at the shell code or malware stages.	
	Solution should be resilient to cases where the shell-code or malware would execute only upon a restart or a shutdown of the end point.	
	Human Emulation: Solution should emulate real user activities such as mouse clicks, key strokes etc.	
	Icon similarity: the solution should be able to identify icon that are similar to popular application documents	
Premium Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, RMA, software updates and subscription update support three (3) years identically same for both the appliances.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should submit the Manufacturer Authorization Letter.	
Professional Service for Planning, Deployment, Migration and Others	Vendor must offer required Professional Service (PS) from OEM (not from SI).	
	Professional Service Engineer will be responsible for following activity:	
	– Understanding procuring entity Network Architecture.	
	– Preparing Network Diagram - include HLD and LLD.	
	– Preparing Project plan.	
	– Preparing deployment plan and migration plan (if required).	
	– Working on deployment and migration activity.	
	– Working with customer for ensuring configuration best practice.	
	– Post deployment knowledge sharing session with customer.	
– Working with partner and procuring entity Team for end-to-end UAT.		
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty & Support	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have Depo in Bangladesh and 24x7x365 Global TAC support	

Technical Specification of IP Telephony (IPT)

38. IP Telephony (IPT)		
IP PABX System		
Feature	Specifications	Compliance
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	-
Brand	To be mentioned by the bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
General Specifications	The network will have SIP based call control architecture with call control functionality centralized or distributed across multiple nodes across WAN for enhanced redundancy.	
	A comprehensive IP based solutions based on a Server Gateway Architecture.All Hardware server & Software including OS with licenses required for solution should be provided from day one.	
	Support for integrated telephony solution for Video conferencing devices, Analog & IP Phones, PSTN gateways over IP architecture.The solution should support integrating Video Infrastructure along with Video endpoints without changing current infrastructure so that Telephony user can take a part of video onference.	
	The solution should offer users the ability to use their UC clients and IP Phones outside of the enterprise (Internet) to make audio and video calls along with IM/Presence with or without VPN.	
	The call control system should support adequate redundancy as required . The Call Control Server should support to be deployed in a active-active configuration. The call control system should support fully redundant solution with NO single point of failure and should provide 1:1 redundancy. Both servers should support be capable of scale requested independently. Future provision should be there that in case of a catastrophic failure of both the servers, a disaster recovery server may be placed to take over control of all locations automatically (no manual intervention) including remote voice gateways connected with the system without disruption of any ongoing calls.	
	<ul style="list-style-type: none"> • Bidder has to provide 200 extension necessary license from day 1. • The system should be scalable up to 7000 extensions on the proposed single hardware. 	

RESTRICTED

	Proposed Solution should have capability from day one for 10 users to register simultaneous 10 devices (hard phone and Soft phone) at any point of time for mobility. Rest all users should be licenses to use IP phone.	
	The solution should allow for business to business (B2B) video calls using SIP, H.323 with other organizations without bypassing existing firewalls.	
	The solution should allow provisioning of gateways with redundant power supplies. Also the complete system hardware and software should support IP V6 from day one.	
System Architecture	The call control system should be fully redundant solution with NO single point of failures & should provide 1:1 redundancy. Both the server should do call processing all the time and act as backup in case of the failure of one server.	
	The call control should support clustering over WAN	
	The proposed system should be Integratable with ACD, IVR.	
	The server and gateway should have dual 10/100/1000 ethernet port.	
	The call control system and gateway should support IPv4 and IPv6 from day one.	
	The system should natively support tenant partitioning so as to comply with regulations for not allowing VoIP (CUG calls) and PSTN calls to be bridged. Any third party applications to manage tenant partitioning should not be quoted in the architecture.	
	The proposed call control server should provide support for standards based SIP IP Phones (Wired & Wireless), Analog Phones, Video Phones, Video Conferencing endpoints and soft clients to provide centralized management and unified dial plan.	
	Conference Bridge—provides software conference bridge resources that can be used by IP EPABX.	
	The system should support an inbuilt reporting tool for calls. Reports that are provided include Calls on a user basis, Calls through gateways, Simplified Call Quality.	
	Should support signaling standards/Protocols – SIP, MGCP, H.323, Q.Sig.	
	CODEC support - G.711, G.729, G.729ab, g.722, iLBC	
	The system should provide the ability to perform tasks in bulk i.e. Add, Remove, Update users, phones, gateways, dial plan etc.	
	The system should support creation of users and their authentication locally and via an integration with LDAP.	

RESTRICTED

	The system should support an inbuilt reporting tool for calls. Reports that are provided include Calls on a user basis, Calls through gateways, Simplified Call Quality.	
	The system should support call admission control to configure number of calls that can be active between locations – intercluster and intracluster.	
	Call preservation – redundancy and automated failure – on call-processing failure. In progress PSTN calls at each of the locations should not be interrupted in the event of any WAN failure or call control server failure.	
	Open API should be provided when required which will help to develop customized IP applications which will integrate with call processing.	
	It is required to provide Survivable Call Control functionality so that the survivable system at the remote location i.e. Media Gateway shall provide fall back call control service in case the remote site loses all connectivity to the main Call Control system placed. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control system.	
Security	All the appliances in the call control system should have dual redundant and hot swappable power supply and fans for high availability.	
	All appliances in the call control system should have hot swappable storage media to ensure high availability.	
	Support for configuration database (contains system and device configuration information, including dial plan)	
	Having inbuilt administration web based administration. No additional thick client for administration on the Admin PC. Should also support HTTPS for management.	
	Access to the system should be secure for the purpose of access over IP network. The protection of signaling connection over IP by means of authentication, Integrity and encryption should be carried out using TLS.	
	There should be provision of defining password aging, one time passwords. Provision shall be available to bar unauthorized user to connect to the system. The system should monitor and report the following types of security \ violation login Violations, authorization code violation Station security code violations etc.	

RESTRICTED

	IP Phones should not support direct, external initiated, connections via HTTP, telnet, FTP, TFTP or any other protocol as means to prevent distributed Denial of Service attack exploitation, except those required for routine firmware upgrades.	
	Role Based Account Management to define different levels of administrator access depending on specific function responsibility	
	The system should support complete encryption capabilities with the ability to encrypt all traffic (media and call control signalling) between IP phones, softphones, call controllers, gateways and all other associated endpoints using a strong encryption algorithm (AES, IPSec and SRTP, for example).	
	All management traffic between the remote console/session and control server should be encrypted (SSH for Direct Command Line Sessions, Interface, HTTPS (SSL) for Web Sessions, SFTP for File Transfer Etc.).	
	Should support SSL for LDAP directory integration.	
	All Hardware server & Software including required OS with licenses required for providing above Security measures must be incorporated.	
System Capabilities Summary	The System should have IP capability for interfacing & Communicating with Voice, Video and Data infrastructure	
	The solution should support a minimum of 7500 IP phones and VC systems per Server by only changing hardware.	
	The architecture should support single Server Clustering to provide scalability to offer support for 30,000 IP devices and also to provide redundancy. All the 30,000 users to be managed in a single database which is managed centrally, no multiple databases.	
	The System should support Alternate Call Routing	
	The System should have GUI support web based management console	
	System backups: The management system should have the provisioning for taking manual as well as scheduling of automatic periodic backup of complete system & data.	
	The System should support Audio message-waiting indicator (AMWI)	
	The System should have Automated bandwidth selection	
	Should support SNMP v2, v3	
	It should be possible to monitor the call control system i.e. system performance, device status, device discovery, CTI applications, voice messaging ports etc.	

RESTRICTED

IM & Presence	Solution should provide a "presence" application for users, so that they can see the availability status of their contacts in their contact list.	
	The common supported status for this application should be available, busy, idle, away etc.	
	Should support the users to see other user's IP phone's on/off hook states	
	The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND) etc.	
	Shall provide support for open protocols like XMPP.	
	Presence based desktop application shall allow escalation of Instant Message to Audio call and further to Video call	
	Should support management of contact list and personal settings from Presence based desktop application	
	Should support click to call, click to Video and click to conference features.	
	The Soft Client should have soft phone capability and should support desktop and iPad based point to point video calls.	
Video Telephony Support	The call control system should provide integrated video telephony features to the users so that user with IP Phone / Soft phone and video telephony end point should be able to place video calls with the same user model as audio calls.	
	The users should be able to transfer video calls as audio calls	
	Call-Server should provide a common control agent for signaling, configuration, and serviceability for voice or video end points.	
	Call control system should handle CODEC and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place.	
End user Features required:	Extension mobility	
	Call forward all	
	Message-waiting indicator (MWI)	
	Privacy	
	Device mobility	
	Do not disturb	
	Hunt groups	
	Dial-plan partitioning	
	Distributed call processing	
	Deployment of devices and applications across an IP network	
"Clusters" of Call-Servers for scalability, redundancy, and load balancing		

RESTRICTED

	Intercluster scalability to 100+ sites or clusters through H.323 gatekeeper	
	Fax over IP—G.711 pass-through and Fax Relay	
	Forced authorization codes and client matter codes (account codes)	
	H.323 interface to selected devices	
	Hotline and private line automated ringdown (PLAR)	
	Interface to H.323 gatekeeper for scalability, CAC, and redundancy	
	Language support for client user interfaces (languages specified separately)	
	Multi-Level Precedence and Preemption (MLPP)	
	Multilocation—dial-plan partition	
	Multiple ISDN protocol support	
	Multiple remote CallServer platform administration and debug utilities	
	Prepackaged alerts, monitor views, and historical reports with Real Time Monitor Tool (RTMT).	
	Real-time and historical application performance monitoring through operating system tools and Simple Network Management Protocol (SNMP)	
	Remote terminal service for off-net system monitoring and alerting	
	Real-time event monitoring and presentation to common syslog	
	Trace setting and collection utility	
	Cluster wide trace setting tool.	
	Trace Collection tool.	
	Multisite (cross-WAN) capability with intersite CAC	
	Q.SIG (International Organization for Standardization [ISO])	
	Video calls to be placed with the same user model as audio calls.	
	Call-Server should support new video end points.	
	SIP Video endpoints which should inherit the functionality of audio calls which gives the user the same call model for both video and audio calls.	
	Call-Server should have the infrastructure to handle codec and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place, single point of administration, management of media devices such as gateways and MCUs.	
	Call-Server should provide a common control agent for signaling, configuration, and serviceability for voice or video end points.	
Manufacturer Part Number	The bidder should submit Manufacturer BOQ of the proposed device including the details Part Number	

RESTRICTED

Manufacturer Authorization	The bidder should be direct Partner of Manufacturer and must provide Manufacturer Authorization Letter	
Datasheet	The bidder should provide Datasheet and CE Certificate with the tender document	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
Warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support. Warranty has to be including all component of IPT System	

40. Rack Server for IPT (qty: 2)		
Item	Specification for Rack Based Servers for IPT	Bidders Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Processors	Rack Server shall have a minimum of one (1) Intel latest generation icelake Processors with minimum 2.90 GHz & 16 cores	
Chipset	Intel chipset compatible with the offered processors.	
Internal Storage	The server should Support upto 24 hot-swappable SAS,NL-SAS and HDD drives .	
	Server should be configured with 16 Nos 600 GB 10K HDD drives	
	The Server RAID HW controller (12G SAS) should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60.	
Memory	Should have at least 32 DIMM slots per server and support minimum up to 3TB of DDR4 3200 MHz memory .	
	The Server should be configured with 96 GB of DDR4 Memory from day one	
	Support for advanced memory redundant technologies like Advanced error-correcting code (ECC) and memory mirroring.	
Network	Should have 2 * 10 GbE (embedded) LAN ports , 2 * Quad port 10 Gb SFP+ network cards with Module for LAN connectivity	
PCIe Slots	Up to 6 PCIe Generation 3.0 slots	
Security	The server should provide cryptographic firmware updates	
	Capable to stop execution of the BIOS	

RESTRICTED

	The server should provide hardware policy based security	
	The server should provide Hardware root of trust	
	The server should provide system lock down	
Ports	Should have the following ports for server connectivity	
	• 1 serial port	
	• 4 USB 3.0/2.0 ports	
	• 1 VGA video port	
Others	Supports hot swappable redundant fans	
	Supports hot swappable redundant power supplies	
	Rail Kit and cable mangement arm to be provided along with the server	
VM	Required Vmware Licenses should be provided with the server	
Warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	
Form Factor	2U Minimum	

41. IP Phone Type 1 (Qty: 140)

Feature	Specifications	Compliance
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
General Features	The phone should support Power over Ethernet IEEE 802.3af class 1/2/3 and should also have AC power adapter option	
	Should feature a LCD display of at least 3.5" for information such as calling party name, calling party number, and digits dialed to be displayed.	
	The phone should have two ethernet ports of at least 10/100 BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.	
	Corporate directory and Lightweight Directory Access Protocol (LDAP) integration.	
	Ready access to missed, received or placed calls (plus intercom history and directories).	
	The phone should support QoS mechanism through 802.1p/q.	
	IP address Assignment by DHCP or statically configured	

RESTRICTED

	Hands-free operation with full-duplex speaker-phone	
	The phone should be a SIP based Phone i.e session Initiation protocol (SIP) supported	
	The phone should support XML based services and applications.	
	The phone should have a distinct LED indicator for message waiting.	
	Should have keys for specific functionalities such as – voicemail, directories, settings, transfer, speakerphone, mute on/off, headset etc	
	Media Encryption (SRTP) using AES	
	Signalling Encryption (TLS) using AES	
	Should support 802.1x	
	Encryption of Configuration Files	
	The phone should have the ability to register to call control server over an internet link with or without VPN.	
	The phone should support IPv4 and IPv6 from day1.	
	The phone should support at least 100 entries for call history i.e. missed, received, placed etc.	
	It should support the following codecs: G.711a/μ-law, G.722, G.729a, iLBC	
	The phone should have RJ9 headset port to connect any standards based headset. The phone should also have a separate headset key	
	The phone also includes the following settings - Display contrast, Ring type, Network configuration, Call status	
	The Phone should support the ability to provide different ringtones for internal and external calls.	
	Should have volume control button for easy volume adjustments for the speakerphone, handset and ringer.	
	The phone should support mounting against a wall	
	The phone should support 2 programmable lines keys.	
	The phone should the following features:	
	Call forward	
Calling Features	ii. Call pickup	
	iii. Call waiting	
	iv. Extension Mobility	
	v. Auto answer	
	vi. Message waiting indicator	
	vii. Music on hold	
	viii. Forced Authorization Code (Account Code/FAC)	
	ix. Conference	
	x. Music on Hold (MoH)	

RESTRICTED

	xi. Corporate directory	
	xii. Auto-detection of headset	
	xiii. Busy Lamp Field (BLF)	
	xiv. Callback	
	xv. Immediate Divert	
Warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	

42. IP Phone Type 2 (Qty: 60)		
Feature	Specifications	Compliance
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
General Features	The phone should support Power over Ethernet IEEE 802.3af class 1/2/3/4 and should also have AC power adapter option	
	The phone should have 2 x 1GE ports, one for the LAN connection and the other for connecting to PC/laptop.	
	Corporate directory and Lightweight Directory Access Protocol (LDAP) integration.	
	Ready access to missed, received or placed calls (plus intercom history and directories).	
	The phone should support QoS mechanism through 802.1p/q.	
	The phone should support 802.11a/b/g/n/ac WLAN enabled enterprise.	
	The phone should provide user the flexibility while using the headset i.e. RJ-9, USB-based, 3.5mm	
	The phone should have atleast 2 multi-purpose USB ports that could be used for charging mobile phones, connecting USB headsets.	
	IP address Assignment by DHCP or statically configured	
	Hands-free operation with full-duplex speaker-phone	
	The phone should be a SIP based Phone i.e session Initiation protocol (SIP) supported	
	The phone should support XML based services and applications.	
The phone should have a distinct LED indicator for message waiting.		

RESTRICTED

Should have keys for specific functionalities such as – voicemail, directories, settings, transfer, speakerphone, mute on/off, headset etc	
Media Encryption (SRTP) using AES	
Signalling Encryption (TLS) using AES	
802.1x support	
Encryption of Configuration Files	
The phone should have the ability to register to call control server over an internet link with or without VPN.	
The phone should support IPv4 and IPv6 from day1.	
Should have min 5" screen with colour display with at least 4 programmable line keys	
The phone should support backlit indicators for the audio path keys (handset, headset, and speakerphone), select key, line keys, and message waiting.	
Should support following audio codec - G.711a, G.711u, G.729a, G.729b, G.729ab, iSAC, Internet Low Bitrate Codec (iLBC), OPUS	
The phone should also have a separate headset key	
Should have a built-in camera with 720p resolution (encode & decode). The camera should have a shutter to open/close camera. Should support standards based video protocol H.264	
Should support self-view video, picture in picture (pip) with adjustable positions of pip.	
Should support Bluetooth (v4.1 LE) for handsfree earphones	
Should support Call history synchronization to view placed and missed calls of mobile device from the IP Phone	
Should support Contact synchronization to synchronize the contacts from the mobile device to IP Phone	
The phone should support mounting against a wall	
The phone should support at least 100 entries for call history i.e. missed, received, placed etc.	
The phone should support the ability to add expansion modules to increase the line capacity i.e. for use by Operators/Receptionists	
Should support busy lamp indicator (BLF) to indicate the presence	
Should support boss-secretary feature, so that secretary can answer calls on behalf of Manager	
The handset should be hearing aid-compatible	

RESTRICTED

Calling Feature	<p>The phone should support the following features at a minimum:</p> <ul style="list-style-type: none"> a. Call forward b. Call pickup c. Call waiting d. Calback e. Call park f. Conference g. Extension Mobility h. Auto answer i. Auto-detection of headset j. Immediate Divert k. Music on hold (MoH) l. SIP URI dialing m. URL Dialing n. Message waiting indicator (MWI) o. Personal directory p. Forced Authorization Code (Account/FAC) q. Call history lists 	
Warranty	<p>Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support</p>	

43. PSTN Gateway (Qty: 02)

Item	Required Specification	Bidder Response
Brand	To be mentioned by the bidder (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Industry Certifications and Evaluations	Proposed solution must be in Leader for Wired and Wireless LAN Access Infrastructure segment in Gartner MQ Last 5 Years	
Environmental	Maintain International Quality Environmental Safety standard	
Enclosure Type	Rack mountable maximum 2 RU	
Router Processor Type	High-performance multi-core processors	
DRAM	Min. 16GB (installed) Max 32 GB Upgradable	
Hardware Capacity	Router should min.19 Gbps from day 1 in 1400 bytes.	
Flash Memory	Integrated Min. 8 GB (installed) Flash Memory	
Interfaces	Router should have Min. 4x1GE WAN & 2-Port FXS and 4-Port FXO Network Interface Module from day 1. Bidder has to provide 4 nos of 1G SFP module from day 1. All SFP should be from the same OEM.	

RESTRICTED

	USB: 2 x USB 2.0 Type A port. Serial: 1 x auxiliary port	
Security hardware:	Hardware-based cryptography acceleration (IPsec)	
Security	Should support Layer 7 context-aware / application aware Firewall features	
	Should support stateful Firewall, transparent firewall, advance application inspection and control for HTTP, ACL bypass and VRF aware Firewall features	
	Should support Up to 2Gbps of IPsec Internet Mix (IMIX) traffic. Should support SDWAN mode & Non SDWAN mode 3900 tunnels. Router should have support IPv4 Routes 1.5 M and IPv6 Routes 1.4 M from day 1. Number of ACL 3900, Number of Firewall session 510K, VRF 3900 from day 1. Router should support strong encryption like AES 256 or higher with hardware-based encryption from day 1.	
	Should support ACL for IPv4 and IPv6, Time based ACL,	
	Should support Dynamic VPN to connect remote VPN devices. "Solution should provide secure intelligent integration with cloud providers like Amazon and Azure and they should able to connect on WAN like any other branch location"	
Interface support	Support Gigabit Ethernet, T1/E1, Channelized E1/T1, FXO, 4G/LTE Service Card	
Supporting Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast Sparse Mode (PIM SM), PIM Source-Specific Multicast (SSM), Resource Reservation Protocol (RSVP), Neighbor Discovery Protocol, Encapsulated Remote Switched Port Analyzer (ERSPAN), IP Service-Level Agreements (IPSLA), Internet Key Exchange (IKE), Access Control Lists (ACL), Ethernet Virtual Connections (EVC), Dynamic Host Configuration Protocol (DHCP), Frame Relay, DNS, Locator ID Separation Protocol (LISP), Hot Standby Router Protocol (HSRP or similar), RADIUS, Authentication, Authorization, and Accounting (AAA), Application Visibility and Control (AVC), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, Multiprotocol Label Switching (MPLS), Layer 2 and Layer 3 VPN, IPsec, MACsec	

RESTRICTED

	Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE 802.1ag, and IEEE 8023ah	
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol, Multilink Point-to-Point Protocol, High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, V.35), and PPP over Ethernet	
QOS Features	QoS, Class-Based Weighted Fair Queuing, Weighted Random Early Detection, Hierarchical QoS, Policy-Based Routing, Performance Routing and network based application detection mechanism	
Expansion Slots	Should have min. 1 Service module & 1 NIM Module slots from day 1.	
High Availability	Support On-Line Insertion (OIR) for Network Interfaces Modules to reduce downtime during fault/repair/upgrade	
	Redundant power Supply from day 1	
Other Features	Support Event Manager for customizable event correlation and policy actions during failure/error threshold exceed	
	Telnet and SSH	
	Support application performance monitoring	
	Should have Network Flow Statistic, Service Level assurance feature. Central management should support bandwidth monitoring including upload and download speed of link and centralize packet capture capability	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details' part numbers and Manufacturer's Warranty letter.	
Training	Bidder must submit the required performance document and compliance reference document for the proposed device.	
Warranty	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support.	

TECHNICAL SPECIFICATION OF SOFTWARE- CDC, DRDC & PC

1. **OS Software.**

a. **Server OS License.**

- (1) Brand : Windows
- (2) Manufacturer: Microsoft
- (3) Version : 2025 Standard Edition
- (4) License : Perpetual License

b. **Server OS License.**

- (1) Brand : Windows
- (2) Manufacturer: Microsoft
- (3) Version : 2025 Enterprise Edition
- (4) License : Perpetual License

c. **Server Client Access License (CAL).**

- (1) Brand : Windows
- (2) Manufacturer: Microsoft
- (3) Version : 2025
- (4) Subscription based for 1 year

d. **Server OS License.**

- (1) Brand : Linux
- (2) Distribution : RED HAT
- (3) Subscription based for 1 year

2. **Security Related Software.**

a. Multi Factor Authentication (MFA) (Subscription: 3 year)		
Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by bidder. (Preferably Cisco)	
Model	To be mentioned by bidder.	
Country of Origin	As per tender specification, article 20	
Country of Manufacturer	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
General Functionalities	The proposed solution should allow users to enroll multiple devices for authentication	
	The proposed solution should support 500 users from day 1	
	The proposed solution should allow users to select a preferred device for authentication	
	The proposed solution should allow users to select an alternative device (provisioned for that user) if their primary device is not available.	
	The proposed solution should allow users to securely manage their devices to reduce administrative workload and it should be configurable on a group and / or application level	
	The proposed solution should support authentication with a push notification to a mobile smartphone.	
	Push authentication should use asymmetric keys to ensure secure communication between the authentication app and the authentication platform	
	The proposed solution should support authentication with passwordless authentication methods by using biometric authentication based on FIDO2 standards	
	The proposed solution should allow admin to enable additional verification to push based authentication. Which generates a verification code from access device and verify the same code on authentication device	
	Authentication App should display information about authentication request like application, location of use, time zone information of access device	
	The proposed solution should support authentication with a SMS method.	
	The proposed solution should support following Mobile Platforms for authentication - iOS & Android	
The proposed solution should support authentication with an out-of-band phone call method for both cell phones and land lines with extensions (ie - not leaving an OTP but		

RESTRICTED

	requiring user interaction)	
	The proposed solution should support authentication with a hardware token	
	The proposed solution should support any third party OATH HOTP compliant hardware token	
	The proposed solution should support third party Yubikey tokens	
	The proposed solution should support authentication with a one-time passcode	
	The proposed solution should provide bypass codes to authenticate	
	The proposed solution should not have any additional user costs for mobile applications	
	The proposed solution should provide a second factor authentication method which can work without any data or network connectivity	
	The mobile applications should support provisioning using a QR code and it should not require a third party QR code scanner	
	The mobile application should support provisioning using a link sent via SMS	
	The proposed solution should support IP Whitelisting and IP Whitelisting should be configurable based upon user/group and/or application type	
	The proposed solution should have single console for management, configuration, and monitoring.	
	The proposed solution should provide automated audit and access logs, reports for any access violation.	
	The proposed solution should have manageability over web application console using HTTPS protocol	
	The proposed solution should intuitively prompt users for all available authentication options when logging in through a web portal. Intuitive web prompt should be configurable based upon user/group and/or application type	
	The proposed solution should support users having redundant authentication devices for flexibility	
	The proposed solution should support U2F like Yubikey tokens for authentication on browser based applications	
	The proposed solution should provide custom reports like based on GEO location, Access Type, Time etc.	
	The proposed solution should not store any users credentials on database	
	The proposed solution should be able to disable/Wipe the token remotely in case of any security incidents.	
	The proposed solution should have inbuilt two factor authentication for accessing management console	
	The proposed solution should support failure mechanism in case solution becomes unavailable	
	Any component of the proposed solution should be deployed on an Windows or Linux VM running on VMWare, Hyper-V or LPAR hypervisor	

RESTRICTED

	The communication between central server and client endpoints irrespective of their location should be secured with encryption	
	The system should allow the administrators to create temporary policies and apply these policies to temporary subset of users in order to validate the settings applied.	
	The proposed solution should use asymmetric cryptography for remote authentication	
Administration	The proposed solution should provide auto provisioning tools to sync existing users from AD	
	The proposed solution should allow for custom policies to restrict the authentication methods available for authentication to control risk based upon group or application (i.e. push, passcode, sms, phone call etc.)	
	The proposed solution should allow users to be added via a CSV import	
	The proposed solution should support admins provisioning users programmatically via Restful APIs	
	The proposed solution should allow admins to enable a self-enrollment process for end users to reduce deployment timeframes. It should be supported for groups/users and/or applications	
	The proposed solution should support admins to enroll and provision users via an email	
	The proposed solution should allow for admins to create a custom enrollment email message	
	The proposed solution should allow administrators to create groups to organize and manage users	
	The proposed solution should allow administrators to limit access for certain integrations/applications based upon user membership for groups	
	The proposed solution should allow administrators to re-active devices for users	
	The proposed solution should allow administrators to generate a one-time use bypass code based upon appropriate rights	
	The proposed solution should allow administrators to limit authentication factors/types for all users globally	
	The proposed solution should allow administrators to limit authentication factors/types for certain groups of users	
	The proposed solution should allow administrators to setup an outgoing caller ID for phone call authentication	
	The proposed solution should allow administrators to control settings for SMS passcodes with regards to # of passcodes sent per request	
	The proposed solution should allow administrators to control settings for SMS passcodes with regards to expiration	
	The proposed solution should support username normalization to control the number of user IDs in the system and optimize licensing (ie- treating	

RESTRICTED

	jdoe@acme.com,acme/jdoe and jdoe as the same user)	
	The proposed solution should support usernames with UPN or NTLM format	
	The proposed solution should support users who may be part of multiple domains	
	The proposed solution should provide the capability to export logs to a third party SEIM	
	The proposed solution should log IP address of login	
	The proposed solution should provide Restful APIs for admin functions	
	The proposed solution should support Role Based Administration Controls for admins	
	The proposed solution should allow for customized branding with corporate logo	
	Administrator must be able to generate all type of reports in csv and jSON format.	
	The proposed solution should provide a configurable lockout threshold for unsuccessful login attempts and the solution should support auto-lockout expiration for configurable time	
	The proposed solution should support proactive reporting on fraudulent login attempts and should be configurable to send the information to admins or a distribution group as email	
	The proposed solution should allow admins to define retention of logs indefinitely or for a specific time period	
Integration	The proposed solution should be able to provide multifactor authentication for Windows, Mac, Linux Operating systems.	
	The proposed solution be able to provide multifactor authentication for VPNs, Firewall, Network Switch's, & Router	
	The proposed solution should be able to integrate with applications supporting Radius protocol	
	The proposed solution should be able to integrate with LDAP solution for user authentication	
	The proposed solution should have a SSO platform that can integrate with multiple Active Directory forests	
	The solution should be able to integrate applications that are using table based identity stores for providing primary authentication	
	The proposed solution should provide multifactor authentication for emails (server & end users) using web clients	
	The proposed solution should provide multifactor authentication for in-house developed application using Auth API or WebSDK's available in different languages	
	The proposed solution should provide multifactor authentication for cloud service providers like Azure, Google, AWS, cloud SaaS solutions Office 365.	
	The proposed solution should offer APIs to either extend or customize the application authentication mechanism	

RESTRICTED

	The proposed solution should integration with Office 365 with Microsoft proprietary federation protocol WS-Trust	
	The proposed solution should be able to integrate with any application supporting SAML 2.0 for authentication and single sign-on experience	
	The proposed should should be able to integrate with any application supporting SAML 2.0 for authentication and SSO experience without having to deploy any SAML server on premise	
	The proposed solution should support SAML 2.0 natively and should be able to integrate with ADFS.	
Licensing	The proposed solution should have a per user cost	
	The proposed solution should not have a per user authentication device cost	
	The proposed solution should not have a per integration cost	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	
Warranty, Subscription & Support Services	Manufacturer's warranty part number Must be mentioned, minimum 03 (Three) years warranty including OEM technical solution support, Patch & New Software Upgrade, RMA replacement Must be provided for this unit from the date of commissioning and services free of cost.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

b. Email security gateway (Subscription: 3 year)

Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender specification, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
Type	To be mentioned by the bidder.	
Form Factor	To be mentioned by the bidder.	
High Availability	Must be Paired High Available.	
General Features Requirement	The solution should be on premise and should support active/active or active/passive High Availability mode.	
	The email security system offering should be dedicated OEM Physical appliance / virtualization appliance based solution and not a subset of NGFW, Proxy or other security solution	
	The gateway should support a comprehensive email	

RESTRICTED

	security solution that integrates inbound and outbound defenses against latest email threats such as Graymail Safe unsubscribing, snowshoe spam, viruses, Malicious URL Blocking, URL category based filtering, Robust anti-APT, DNS RBL verification, reputation filtering, DLP, Encryptions and phishing filtering utilizing a strong global threat intelligence capability	
	The solution should support minimum 600 users for anti-spam, anti-virus, virus outbreak, data loss prevention and encryption, Anti-APT, Graymail, phishing etc. All features required from day one.	
	The solution should have false positive efficacy of 1 in 1 million	
	Propose solution should not be software- based and installed in the mail server. It should be purpose- built dedicated email security gateway.	
	The solution should have the capability to force an SMTP over the TLS connection when sending emails to or receiving emails from a specific domain.	
	The solution should support ability to perform SMTP session control and traffic rate limiting according to sender's IP address/range, domain or email reputation. The solution should be able to assign maximum SMTP sessions per IP address on appliance	
	The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack), directory harvest prevention, and have ability to perform SMTP session control and traffic rate limiting (down to per recipient) according to sender's IP address/range, domain or email reputation.	
	The solution should have the ability to utilize a database of IP addresses and domain pairs to help block spam and allow good email through, similar to a Registered Email Sender List (RESL).	
	The solution should be able to block bounce messages/NDR from forged return addresses that did not originate from your network.	
	The solution should have the ability to enforce email policy based on the character set of message parts.	
	The solution should be able to perform a reverse DNS lookup on the sender IP address, determine the Top Level Domain (TLD) and block emails originating from IP addresses assigned to providers in common spamming countries.	
	The solution should be enable administrators to create custom rules based on results of reverse DNS lookup of sender IP address.	
	The solution should be able to enforce email policy by checking the name server of a domain referenced in an embedded URI and validating against a list of name servers known to be used exclusively by spammers.	

RESTRICTED

	<p>The solution shall provide the following features:</p> <ul style="list-style-type: none"> a) Preferable with Data Leak Prevention b) Per-User Quarantine Setting c) Sender ID checks d) Role based Access (Console) e) End User Quarantine Capability (Per user or globally) viewing and releasing f) Spam/Spoofing inspection/protection g) Email Anti-Virus & Anti-Malware h) Email Outbound Filtering i) Content Filtering j) Protection and inspection against fake messages, executable files, Malicious code, scripts, Bounced/newsletters/graymail/marketing and social network messages 	
	<p>The solution should be able to enforce email policy by inspecting the content of free Web sites such as GeoCities and Blogspot linked to URIs in spam emails.</p>	
	<p>The solution must be able to prevent spammers from sending large amounts of emails to the appliance over a short time period from any single IP address.</p>	
	<p>The solution should be able to receive email from IPv6 networks, apply content policies, and deliver to either IPv4 or IPv6 networks.</p>	
	<p>The solution must be able to prevent compromised internal systems from sending emails to a large number of recipients from a single user account over a short period of time.</p>	
	<p>The proposed solution should support centralized reporting and message tracking after the aggregation of data from multiple email security appliances. Message tracking data should be aggregated from multiple email security gateways, including data categorized by sender, recipient, message subject, and other parameters.</p>	
	<p>The solution should provide forged email detection protection against business executive compromise and provide detail logs on all attempts and actions.</p>	
	<p>The solution should support policies to sign outgoing emails based on domain key and allow to sign by different domain keys based on sender domain</p>	
	<p>The solution should support outbound SMTP over TLS based on destination domains or system wide and support outbound SMTP authentication</p>	
	<p>The solution should certificate management capabilities for S/MIME encryption and/or digital signatures including support for access to public key repositories, ability to harvest public keys from received emails, and export/import of public keys both individually or in bulk.</p>	
	<p>The solution should support to selectively apply digital</p>	

RESTRICTED

	signatures on outbound emails including capability to apply digital signatures based on policy using mail or other attributes.	
	The solution should support for adding DKIM signatures on outbound email including the capability to selectively apply DKIM signatures based on policy and apply different DKIM signatures based on policy or domain.	
	The solution should support for SPF, DKIM, and DMARC email authentication including ability to apply email authentication requirements based on domain (specific or wildcard), ability to quarantine emails failing authentication, DMARC reporting, and any other authentication policy features. Include ability to selectively confirm email authentication success (SPF, DKIM, DMARC) for inbound messages on other filtering policies that may include white listing of those addresses.	
	Appliance should have DLP feature with full template based DLP, so that organization can deploy DLP as per their compliance and require database.	
	Multi-layer Anti-spam filter: TCP connection level Reputation Filtering (Sender IP/domain) On Box Anti-spam Filtering allow integrated use of different vendor anti-spam engine the spam rules should be automatically updated every 5 minutes. Solution should be able to distinguish between spam and marketing mail from a legitimate source	
	The solution should support following for system monitoring: - SNMP v2/v3, MIB-II, XML, Syslog support	
	The solution should support authenticate users using RADIUS or LDAP and two-factor authentication for secure access into appliance for management purpose	
	The appliance should support the use of IPv6 for: a) Appliance interfaces b) Gateways (default routes) c) Static routes d) SMTP Routes e) Querying external SMTP server with IPv6 address (for Recipient validation) f) IPv6 Sending hosts g) Content Filters h) Sending to IPv6 destinations i) Report searches	
	The solution should support configuring appliance to scan for URLs in message attachments, and perform configured actions on such messages if malicious.	
	The solution should be able to consume external threat information in STIX Format communicated over TAXII Protocol	
	The solution should be able to integrate with Domain Reputation Service that provides a reputation verdict for	

RESTRICTED

	email messages based on a sender's domain and other attributes.	
	The solution should support DNS-based Authentication of Named Entities (DANE) for outgoing TLS connections on your appliance.	
System Performance	The solution must offer a layered approach to scanning email, using both connection management and mail scanning techniques to filter email.	
	The solution should be scalable up to 10,000 active email users from day one & should support up to 5000 domains.	
	The solution must have Advanced Threat Protection license from day 1 to mitigate ZERO Day attack from OEM cloud	
Anti-spam Features	The proposed solution should support spam quarantine on the centralized appliance. Holds spam and suspected spam messages for end users, and allow end users and administrators to review messages that are flagged as spam before making a final determination.	
	The proposed solution should have the Multi-layer Anti-spam filter: It should have the capability to scan emails for spam with 3rd party SPAM engine before the OEM Spam engine.	
	The solution should offer users the ability to whitelist/blacklist senders as well as manage their own spam scores.	
	The solution should have the ability for administrators to block emails via header/subject/body using regular expressions and exact word matches.	
	The solution should be able to block attachments by file type and file extension.	
	The user intervention should not be required to install/update spam, virus, and security definitions.	
	Message delivery options should include - Inbound and outbound (unless specified): a) Discard b) Deliver immediately c) Reject (outbound) d) Quarantine e) Add banner f) Tag the subject and continue	
	The solution should block phishing URLs including targeted spear phishing attacks	
	The solution should convert any types of URL link to plain text that contains in the mail body.	
	The solution should offer users the ability to whitelist/blacklist senders as well as manage their own spam scores.	
	The solution should offer Per User Scoring Setting	
	The solution should offer-size based as well as age-based retention for storing user's quarantined messages	

RESTRICTED

	The solution should offer separate queue for outbound quarantine emails	
	The solution should offer GRC account/role only has access to Outbound Quarantine and can decide which messages to deliver, reject or delete based on DLP/content policy.	
	The solution should have dedicated RBL	
	Proposed solution should offer separate tab for ATP logs	
	The solution should offer an option to block or quarantine messages based on country of origin or language	
	Must offer Bayesian Analysis	
	Must offer Spam scoring - URL Reputation within email messages	
	The solution should offer SPF & DKIM Check - Directory Harvest Attack (DHA) protection	
Anti-Virus and Malware Protection Features	The solution must offer multilayer layers of antivirus protection.	
	The solution should have dual virus scanning available within the appliance. one of the AV engine should be from Gartner leader/Challenger quadrant	
	The solution should provide protection against zero-day and targeted attacks. It should be able to dynamically analyze message attachments for malware without sending files to cloud	
	The proposed solution should include Anti-APT/Next Generation detection ability to quarantine emails suspected to be infected with malware both for inbound as well as outbound email	
	The proposed solution shall support the ability to hold the email until sandbox analysis is complete and the threshold shall be configurable	
	To proactively respond to cyber threats such as malware, ransomware, phishing attacks, solution should have capability to consume external threat information in STIX/TAXII	
	The solution should provide virus outbreak prevention on abnormal increase of emails with specific email attachments	
	The solution should support the scanning of URLs in message attachment and perform action on such message.	
	The solution should provide capability of the appliance to perform recipient validation by querying an external SMTP server prior to accepting incoming mail for the recipient	
	The solution must offer real-time protection that will block new spam and viruses in real-time without waiting for new definitions to be downloaded to the appliance.	
		The solution must cache definitions for known viruses locally
	The solution should be able to provide internal email	

RESTRICTED

	antivirus protection.	
Quarantine Features	Full quarantine access for Administrator or delegated Quarantine access.	
	Individual User/Password Access Control for spam Quarantine Area	
	End User Quarantine Support with LDAP/AD/IMAP/POP authentication support	
	The solution should provide separate Quarantine areas for different functionalities such as: a) Dedicated Spam Quarantine to quarantine spam/suspect- spam b) Virus Quarantine – to quarantine virus files c) Outbreak Quarantine – Dynamically quarantine zero day threats d) Policy Quarantine – to quarantine based on policy such as “quarantine outbound Resume’s” e) Flexibility to create additional Policy quarantines f) End user can read, release, whitelist, blacklist from self-quarantine folder.	
LDAP Support	The solution should support: a) LDAP routing b) Masquerading c) Recipient address verification d) SMTPAUTH using LDAP	
	LDAP should be query based and not synchronization based for better performance.	
	The solution should support chained LDAP queries that will run in succession.	
	The solution should support LDAP referrals i.e. When using LDAP referral’s, the original query gets referred to another LDAP server.	
	The solution should support LDAP caching on the appliance.	
Email Encryption Features	Proposed solution must support email encryption from day 1 without additional license	
	Solution should be able to do outbound email encryption through policy on the unit or user specified.	
Content Detection and Analysis	The proposed solution shall support mime and file-type detection technology	
	The proposed solution shall support: a) Comprehensive data-loss prevention with custom content policy. b) Healthcare, Finance, personally identifiable information c) PDF Scanning and image analysis d) Dynamic Adult Image Analysis Service to identify and report or block the transmission of adult content	

RESTRICTED

	e) Intent analysis f) Image analysis	
3rd Party Integration/API	The proposed solution must provide integration with Active Directory for recipients address validation	
	The proposed solution must have option to integrate with 3rd party via API	
	The proposed solution is preferable to be integrated with SIEM solutions.	
Reporting and Log Search	<p>Solution must offer multi types of reports that can be generated on demand and emailed to the administrator and should have but not limited to:</p> <p>a) Real-time reporting capabilities b) Dashboard visibility into message logs c) System reporting d) Email Virus detection/stoppage reporting Spam Detection reports e) report scheduling capabilities f) ATP reporting g) Reports exportable in multiple formats</p>	
Administration and Management	The proposed solution should offer Outlook Plug-in support for reporting missing spam, false positives, virus emails, encryption etc.	
	The proposed solution support both Internet Root DNS servers or local DNS servers	
	The proposed solution support multiple DNS servers according to destination domain(s), i.e. DNS A server for Domain A, and DNS B server for Domain B	
Warranty & Support	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) year warranty for technical solution support with Patch & New Software Upgrade should be provided for the proposed solution. .	
	The OEM should have local office & Depo in Bangladesh	
	24x7x365 Global Technical Assistance Center/Technical Support and Assistance Center.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

c. Extended Detection and Response (XDR) (Subscription: 3 years)		
Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by the bidder. (Preferably Cisco)	
Model	To be mentioned by the bidder	
Country of Origin	As per tender spec, article 20	
Environmental	Maintain International Quality Environmental Safety Standard	
General Requirements	The proposed solution should support the use of a browser for monitoring and administration purposes. Traffic should be encrypted (via SSL) between the browser and the proposed solution	
	The proposed solution should support 600 users from day 1	
	The proposed solution should support role-based security by restricting all or portions of system/sub-system access to authorized groups and individual users.	
	The proposed solution should provide a dashboard which shows a high-level summary of the incidents within the organisation	
	The proposed solution should support the creation of custom dashboards, allowing security analysts to display selected metrics and data from integrations	
	The proposed solution should understand the impact of a threat, discover the scope of the breach, and take single-click actions from one interface.	
	The proposed solution should provide a mission control view for metrics and data across the entire security environment. The interface should allow the user to create custom dashboards and tiles to display metrics and data from integrations.	
	The proposed solution should consolidate inventories from integrated data sources and third-party Sources and provide a unified view of the devices and users in the organization.	
Integrations	The proposed solution should support integration with EDR (Endpoint Detection and Response) products for Threat Hunting & Investigation. Provide a list of EDR products which integrate with the proposed solution to support these capabilities	
	The proposed solution should support integration with EDR (Endpoint Detection and Response) products for Threat Containment (e.g, Isolate an malware-infected endpoint). Provide a list of EDR products which integrate with the proposed solution to support these capabilities	
	The proposed solution should support integration with	

RESTRICTED

	EDR (Endpoint Detection and Response) products for Asset Inventory and Context to help triage detected threats. Provide a list of EDR products which integrate with the proposed solution to support these capabilities	
	The proposed solution should support integration with NDR (Network Detection and Response) products to enrich observables during an investigation. The enrichment may include reputation information, reported sightings about the queried observable. Provide a list of NDR products which integrate with the proposed solution to support these capabilities	
	The proposed solution should support integration with Email Security/Protection products to enrich observables during an investigation. The enrichment may include reputation information, reported sightings about the queried observable. Provide a list of Email Security/Protection products which integrate with the proposed solution to support these capabilities	
	The proposed solution should support the ingestion of endpoint telemetry to provide visibility on an endpoint's behaviour both on-premise and off-premise. The collected telemetry would include information about the flows from the endpoint along with context like user logged in, process associated with network connections, Operating System, etc.	
	The proposed solution should be integrated with Threat Intelligence. Provide a list of Threat Intelligence sources which integrate with the proposed solution to support these capabilities.	
Threat Detection	The proposed solution should support integration with EDR, NDR, NGFW, Email Security, IAM and Public cloud platforms to correlate threats across vectors.	
	The proposed solution should utilize behavioral modeling, multilayered machine learning, and global threat intelligence to detect threats on-premises and in the public cloud environments.	
	The proposed solution should automatically classify entities into roles by observing traffic and config information without user intervention.	
	The proposed solution should Identify threats in encrypted traffic without compromising privacy and data integrity.	
	The proposed solution should detect threats with confirmed detections and provide multiple points of enforcing remediation controls, beyond just the endpoint.	
	The proposed solution should have the capability to natively detect the following threats:	
	a) Command & Control activity	
	b) Brute force detection	
c) Potential data exfiltration		
d) DDoS and Network floods		

	e) Reconnaissance and scanning	
	f) Lateral movement	
	g) Cryptographic connections using weak encryption methods	
Incident Management	The proposed solution should support risk-based prioritization of security incidents, so that security analysts can focus on the most critical incidents impacting the organization. Provide a brief explanation of how the risk-based prioritization of incident is achieved.	
	The proposed solution should provide the following details of an incident:	
	a) Status of incident (e.g. Open, Closed, Rejected, Containment-Achieved, etc)	
	b) Who has been assigned to the incident	
	c) Which security solution reported the incident along with the timestamp	
	d) Description of the incident	
	e) MITRE ATT&CK Tactics associated with the detections in the incident	
	The proposed solution should provide a simple, single-page high-level Overview of an incident with the information:	
	a) An attack graph which shows possible paths of attack against the organisation's infrastructure	
	b) Assets (e.g. endpoints, devices, etc) which are involved in the incident	
	c) Observables (e.g. IP Addresses, Domains, URLs, File-Hashes, etc) related to the incident. These observables should include associated dispositions (e.g. Malicious, Suspicious, Unknown, etc). Each observable should also be colour-coded to allow the security analysts to easily distinguish the observable type.	
	The proposed solution should automate triage and prioritization of alerts from other security portfolio solutions in order to improve SOC productivity.	
	Incident Response & Automation	The proposed solution should support a step-by-step guided response to help a security analyst respond to an incident based on best practices aligning to the NIST 800-61r2 model format (Preparation, Detection and Analysis, Containment, Eradication, Recovery, and Post-incident) produced by SANS Cybersecurity Training Organization.
The proposed solution should include an audit log of changes to an incident during its lifecycle. These changes should at a minimum include action taken, timestamp, description and apply to incident assignments, status updates, workflow actions.		
The proposed solution should provide a no-to-low code approach for building automated workflows that can leverage third-party multi-domain systems, applications,		

RESTRICTED

	databases, and network devices in the environment to create workflows.	
	The proposed solution should allow customization and creation of custom response actions and workflows	
	The proposed solution should provide a list of pre-written workflows that have been released or approved by OEM engineers and content providers. Desired workflows should be able to be viewed and installed, as required.	
	The proposed solution should allow the ability to define a particular workflow into a pivot menu of any observable throughout the solution matching the type(s) that was selected.	
	The proposed solution should provide a capability that enables workflows to communicate with resources inside the network that are not exposed to the internet in order for the workflows to interact with on-premises components.	
Threat Investigation	The proposed solution should support investigative capability to search for suspicious indicators of compromise (IOCs) such as emails, log messages, domains, URLs, and IPs, and extract observables for enrichment.	
	The results of an Investigation should display a 2D Relations Graph - showing how the observables (e.g. Domains, URLs, Ips, etc) in the investigation are connected.	
	The results of an Investigation should also show a colour-coded sightings timeline (based on disposition) of when the observables in the investigation were first and last seen in the organization's environment	
	The proposed solution should provide an option to save the results of an investigation. Saved investigations can provide evidence to justify a course of action.	
	The proposed solution should provide an interface that aggregates context from security solution data sources along with global threat intelligence from Talos® and third-party sources via APIs.	
Management	The proposed solution must be available as a fully managed (vendor supported) offering or locally managed.	
	The proposed solution must support Single Sign On (SSO) and Azure AD for user management.	
	The proposed solution must support data retention for telemetry at a minimum of 90 days and extendable beyond with the purchase of additional licenses.	
	The proposed solution must support configuration and deployment of a next generation client with a Cloud Management solution in a single, unified end-user interface.	
Manufacturer's part number	Bidder should submit BOQ of proposed device including the details part numbers	

RESTRICTED

Warranty, Subscription & Support Services	Minimum 3 (Three) years warranty for OEM, Manufacturer's warranty part number should be mentioned. The OEM should have local office & Depo in Bangladesh and 24x7x365 Global TAC support	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	
d. SIEM (security information and event management) and SOAR (security orchestration, automation, and response) (Subscription: 3 years)		
Item	Product Specifications	Bidder Response
Quality	ISO 9001/9002 for manufacturer, FCC Class A/B for quality assurance	
Brand	To be mentioned by bidder. (Preferably Cisco)	
Model	To be mentioned by bidder.	
Country of Origin	As per tender specification Article no 20	
Country of Manufacturer	As per tender specification Article no 20	
Environmental	Maintain International Quality Environmental Safety Standard	
General Specifications	The proposed solution must include Next Gen SIEM, Security Analytics, SOAR Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM, & SBDL	
	The proposed solution should be sized for 150 GB/Day sustained at all layers and should be scalable upto 300 GB/day without dropping or queuing of logs as per customer requirement. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	
	To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. Each index/ virtual storage group should be used for searching specific data and retention period should be configurable as per indexes.	
	The proposed solution must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	
	The proposed solution should provide a test/dev license as part of the solution. It should also provide a tool in-built or integrable, that allows to create test bed environment which can help to simulate blue team and	

RESTRICTED

	red team attacks to test use cases, train analysts etc.	
	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.	
	Machine learning should be embedded across the platform (SIEM, SBDL). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	
	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period of online 180 days and 365 days of archival. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re-ingesting security analyst would save storage cost and identify and pinpoint attack intime.	
	The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques.	
	should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time.	
	Log Filtering – Not all logs are needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.	
	The proposed solution should have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.	
	The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.	
	The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The Dashboard should be accessible from the endpoints as & when required.	

RESTRICTED

	The Proposed solution must offer all the below built-in threat detection techniques out of the box:	
	Detect Web Application Threats.	
	Detect APT Threats	
	Integrate with any Honeypot/Deception solutions	
	Integrate with any NBAD tools	
	Detect threats indicated by advisories	
	Give visibility of endpoints also by integrating with EDR, Antivirus etc. for endpoint analytics.	
	The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should also be capable of being used for SBDL & SIEM.	
	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	
	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per customer requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.	
	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.	
	The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution.	
	The proposed solution must be software based allowing flexible deployment models and architecture.	
Supported Data Sources	The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs and interfaced incl. text, XML, JSON and other evolving format.	
	The proposed solution must be able to read data input from the following log file formats:	
	a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure)	
	b. Windows Events Logs	
	c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange)	

	servers, DNS servers, DHCP servers, Active Directory servers, etc.	
	The proposed solution must be able to accept the following indicative data streams feeding through the network:	
	a. Syslog Messages	
	b. Security Alerts	
	c. JSON streaming over HTTP/HTTPS	
	The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI	
	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.	
Index, Search, Filter, Analyze and Investigate	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem.	
	Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console whether this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.	
	The proposed solution must be able to build an unstructured index or store data in its original format without any rigid schema.	
	The proposed solution's licensing should be based on post filtering of events. If log events are filtered, then they should not be counted in license.	
	Proposed solution should forward data to multiple destinations apart from its own SIEM processing/data storage layer. Log collector should be able to forward data to multiple destinations.	
	The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events.	

Monitor, Alert and Reporting Functions	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.	
	The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.	
	The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.	
	The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.	
	The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, megabytes, absolute value functions, highest integers, standard deviation, command length etc.; Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.	
	The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs.	
	IndicativeUse Case: Predicting Malware spread based on previous malware attack patterns.	
	The proposed solution must possess built-in function for Predictive Analysis:	
	a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances	
	b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results IndicativeUse Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.	
The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance		

RESTRICTED

	and capacity bottlenecks and outliers in Unix and Linux environment. It should quickly compare resources and capacity utilization across many hosts	
	Indicative Use case: Visibility of services running on servers are also critical to monitor. These could be impacted due to any security incident. Overall performance of the system may get impacted etc. Hence if a SOC analyst have all this view from central platform, then this helps to reduce the time to identify and fix any issue.	
	The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard.	
	Indicative Use Case: To have a single view of entire customer by integrating with NMS and other tools giving the security posture & IT posture status to track issues and fix them immediately.	
	The proposed solution must possess built-in feature for anomaly detection:	
	a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances	
	b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results	
	The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment	
	Indicative Use Case: To have a Single dashboard which can help analyst to identify the real cause of performance degradation which could be due to a security issue or due to any other IT issue.	
	The proposed solution report or table must be able to be embedded in third-party business applications incl. Email, SharePoint, Word Press, Wiki, Whatsapp etc.	
Machine Learning	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	
	The proposed solution machine learning capabilities must include API access, role-based access controls for machine learning models.	
	The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open source libraries like NLP,	

	Python etc.	
	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.	
Search and Reporting	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And Out of box aging analysis of incident should be available.	
	The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing URL parameters to any third party website. The Report should be scalable IP-wise, device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.	
	The product internal logs must be ingested within the product for ease of troubleshooting and investigation and those logs do not consume the product license.	
	The solution must provide granular license utilization down to devices, log sources and data store or additional lookups of devices to agencies by the minute and the retention of granularity can be extended to the project requirement.	
	The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.	
	The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.	
Fields, Schema and Log Parsing	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization.	
	Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time.	
	The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface.	
	The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation	

RESTRICTED

	with existing live or historical data within the system from the web interface.	
	Old data should be parsed with new parser without re-ingesting or re-indexing the data.	
Security Analytics Platform	The proposed solution must provide the following capabilities as a Security Analytics Platform:	
	a. One single syntax that can be used universally for search queries, alerts, reports or dashboards, SIEM, SBDL.	
	b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure	
	c. Risk management technique to apply risk scores to any asset or user based on relative importance or value to the business	
	d. Threat intelligence technique that automatically collect, aggregate, deduplicate indicators of compromise from threat feeds	
	The proposed solution must be fully integrated with the log platform without the need to duplicate the collected raw logs.	
	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.	
	The proposed solution must be able to assign any arbitrary risk score based on self defined query based on any correlated events, statistical analysis, threat indicator match. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.	
	The proposed solution must be able to retrieve from any threat feeds without restriction, retrieve threats in various ASCII/UTF- 8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and Open IOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated exchange of Indicator Information (TAXII).	
	The proposed solution must be able to support the following indicative list	
	Network	
	HTTP Referrer, User Agent, Cookie, Header, Data, URL	
IP		

RESTRICTED

Domain	
Endpoint	
File Hash, Name, Extension, Path and Size	
Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data	
Process Name, Arguments, Handle Name, Handle Type	
Service Name, Description	
Certificate	
Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm	
Email	
Email Address, Subject Body	
Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioral based use cases.	
Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time	
The proposed solutions should use Using distance formula to detect geographically improbable access	
The proposed solutions should use randomness to measure domain names that can be potentially from malware domain generated algorithms.	
Indicative Use Case: Detect DGA using randomness. Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names hence above methodologies are required in proposed solution to detect such attacks	
The proposed solution should use statistic functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases.	
Other analysis:	
Find common or rare events using cluster or most commonly and widely used means clustering method Find percentage of times two fields exist in the same events correlating all the fields.	
Indicative Use Case: Analyst should be able to see an overview of the co-occurrence of fields in data. It should give the percentage of times that the two fields exist in the same events. This will help analyst to see the relationship among all the fields in a set of results	
The proposed solution should find relationship between pairs of fields by change in randomness in pair of fields.	
Indicative Use Case: This helps to predict the value of another field by knowing the value of one field.	
The proposed solution's detection use cases should be	

RESTRICTED

	comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following:	
	ATT&CK MITRE, an adversary behavior model that describes the actions an adversary might take.	
	Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective.	
	CIS Critical Security Controls	
	Data types that are referenced within the rules/search and that need to be populated.	
	Technologies, example technologies that map to the data types.	
	There should be template to upload advisories in an automated manner.	
	There should be templates to design and trigger work flows automatically.	
	Any other customizable templates as per customer requirements.	
	The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)	
Incident Response	The proposed solution must provide investigation auditing capability to enable analysts to easily:	
	Track searches and activities	
	Review activities at any point	
	Select and place into timeline for temporal analysis	
	Help remember searches, steps taken, provide annotation support	
	The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.	
	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.	
	The proposed solution should have integration with major commercially available tools OOTB for triggering actions without dependency with SOAR solution.	
	The proposed solution should be integrated with existing SOAR solution.	
	The must be able to monitor all the users in the organization. should not have separate data repository and should consume and operate on data lake or SIEM data repository.	
	Use Case: Every single user can be source or a target of threat hence it's very important to cover all the users with solution.	
	The must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional	

RESTRICTED

	<p>baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques.</p>	
	<p>Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats.</p>	
	<p>The proposed solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time.</p>	
	<p>Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increase the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations.</p>	
	<p>Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user.</p>	
	<p>The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior.</p>	
	<p>The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat.</p>	
	<p>Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to -specific fields.</p>	
	<p>The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors.</p>	
	<p>The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI.</p>	
	<p>The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain.</p>	
	<p>The proposed solution should find deviations from typical behavior or detection of interesting patterns like beaconing.</p>	
	<p>The proposed solution should detect threats using graph-</p>	

RESTRICTED

	based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity.	
	The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	
SOAR Functionality	The offered SOAR should have bidirectional integration either existing SIEM such that all the actions taken on the SOAR should be visible in incident management of SIEM deployed at customer premise	
	The proposed solution must have a orchestrator ability to direct and oversee all activities from beginning to end with 2 user license.	
	The proposed solution orchestrator must be able to ingest security data from any source and in any format. Example: Email based alerts SIEM based alerts	
	The proposed solution orchestrator must be able to poll data sources or pull data into the platform.	
	The proposed solution orchestrator must be able to interpret the data and make it usable by the platform. Example: extracting indicators from emails	
	IP address Domains	
	File Hashes	
	The proposed solution orchestrator must be able to initiate automation upon creation of new events with artifacts or existing events with new artifacts without human intervention.	
	The proposed solution orchestrator must be able to dispatch automation tasks from it's queue at the appropriate and optimal time, passing them to the automation engine for execution.	
	The proposed solution orchestrator must be able to introduce human supervision if necessary, pausing the automation engine for an approval by asset owner is needed to execute a security action on a target.	
	The proposed solution orchestrator must ensure output data from one action is properly parsed, so that future actions can make use of it.	
	The proposed solution must provide a built-in visual automation editor.	
	The proposed solution built-in visual automation editor must enable users to construct comprehensive and sophisticated playbooks to fully validate, investigate and resolve incident using drag and drop capabilities visually without needing the expert ability to code.	
The proposed solution built-in visual automation editor must be able to represent code using blocks and blocks can be connected in a one-to-one, one-to-many and many-to-one fasion to dictate an order of execution.		

RESTRICTED

	The proposed solution built-in visual automation editor must be able to provide an interface where testing and debug can take place allowing transition from edit mode to test mode	
	seamless.	
	The proposed solution should have built in functionality for triage health check failures – perform ping test, gather information (VM status, OS uptime, SCOM status for Windows), and triage	
	issues.	
	The proposed solution should support periodic automations – notify the users of underutilized VMs and reduce VM profile.	
	The proposed solution should fix a problematic server (Start/Stop/Restart Service) – disable server in Load Balancer (LB), wait for connections to drain, restart, check server health and enable server in the LB.	
	The proposed solution should support disk space remediation - execute steps to cleanup disk when disk space is low, if necessary, increase the disk space within the user specified constraints.	
	The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousand of point products available in the security market today.	
	The proposed solution must provide easy transition in and out of other security technologies without negatively impacting automated playbooks.	
	The proposed solution must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.	
	The proposed solution must standardise on one language like Python for developing integrations with other technologies for custom actions and custom handling of playbooks confined in a block while retaining the original visual playbook editor functionality for the entire playbook.	
	The proposed solution must have documented REST API access that allows full control over the platform.	
	The proposed solution must have ability to label the nature of the event.	
	The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.	
	The proposed solution must be able to extract and store attachments from ingested emails.	
	The proposed solution must have the ability to mark artifacts as evidence.	
	The proposed solution must be able to provide an indicator view to quickly pivot investigation of an indicator	

RESTRICTED

	to past incident occurrences.	
	The proposed solution should provide recommendations on users, playbooks, and actions that can be used to resolve an event.	
	The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.	
	The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions.	
	The proposed solution should have an out of the box guidance by offering suggestions to help investigate, contain, eradicate, and recover from a security event, allowing newer analyst to take and validate choices of more experienced analysts.	
	The proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.	
	The proposed solution must provide central management of incidents and administrative	
	functions from a single web based user interface.	
	The proposed solution must provide multi-tenancy support allowing multiple departments or business units to use the same solution with appropriate segregations/separations.	
Virtual Appliance Requirement	In order to deploy the proposed solution bidder has to include servers with 210 vCPU, 250GB RAM and storage as required to deploy OS as well as 180 days data retention. Relevant OS has to be included in the bid	
Warranty & Support	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) year warranty for technical solution support with Patch & New Software Upgrade should be provided for the proposed solution. .	
	The OEM should have local office & Depo in Bangladesh	
	24x7x365 Global Technical Assistance Center/Technical Support and Assistance Center.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

3. Access Control Software for Servers.

a. Privileged Access Management (PAM) (Subscription: 1 years)		
Specifications	Description of Requirements	Bidder's Response
Brand	To be Mentioned by the Bidder (Preferably MasterSAM/Arcon)	
Model	To be Mentioned by the Bidder	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
General Requirements	The proposed solution provide integrated platform for the following functions into single cohesive solution suite: - Password management - Privilege access management - Granular access control - Surveillance logging - Compliance check	
	The proposed solution must provide one central management console for privileged access, password & access control management and another central log repository management for compliance & surveillance review audit to enforce segregation of roles effectively.	
	The proposed solution should enforce end- to-end accountability effectively with every privileged user is accountable to his/her activity on the system; no hiding behind anonymous ID (e.g., root or administrator) is allowed.	
	The proposed solution should provide superior surveillance logging & recording facility to enforce full disclosure & transparency where none can escape surveillance monitoring; whether from local console or remote network access.	
	The proposed solution should enforce least privileged access at all time, every user is a normal user, until his privileged access has been escalated with independent approval(s).	
	The proposed solution must prevent leap frogging.	
	The proposed solution must be able to enforce segregation of roles & duties with host based granular access control capability.	
	The proposed solution must provide flexible and expandable Combined deployment architecture to support the following deployment methods seamlessly in one single integrated solution platform: - Host based - Gateway/Proxy based - Endpoint based	

RESTRICTED

The proposed solution must be supported licensing Mode like that: 1) Agent Less Platform must be supported Single Production License with Single Disaster Recovery License. 2) Agent Based Platform must be supported Single Production License with Single Disaster Recovery License.	
Proposed PAM Solution should be supported to manage Track and Record minimum 500 User, 250 Resources and 50 Agent.	
Proposed Solution should not have any dependency on Third party Agent and third-party Proxy. The solution must be a single OEM solution.	
The proposed solution should provide integrated management console to manage & support both agent base & agentless set up in its deployment architecture	
Physical and virtualized environment: The proposed solution should be flexible to be hosted under physical or virtualized environment.	
Disaster recovery capability: The proposed solution must come with the technology component to support disaster recovery situation.	
Active directory: The proposed solution should support user authentication via the existing Active Directory.	
The proposed solution must be able to scale up in performance via simple upgrade of standard hardware resources (e.g., RAM, HD, CPU, ...) which are commonly available; as such proprietary hardware is not recommended.	
The proposed solution should provide easy & intuitive web-based configuration by grouping of user or server.	
The proposed solution must provide web- based centralized admin & management capability.	
The proposed solution should support comprehensive web-based request-approval workflow management.	
The proposed solution should be configurable for request-approval matrix to granularly delegate approval authority according to operations & security requirement.	
The proposed solution should be able to support configurable up to 3 level approval with a choice for it to be in sequence or in parallel.	
The proposed solution should allow configuration in duty-segregation manner that different approver(s) is appointed for different request(s).	
The proposed solution should support email approval workflow.	
The proposed solution must be flexible to provide emergency access workflow, e.g., during off-working hour, authorized admin is allowed to submit request which will get auto-approved but limit to short period of time (e.g., 1 to 3 hours), to streamline operation support.	
Real time alert must be triggered when someone uses	

RESTRICTED

<p>this emergency access workflow.</p>	
<p>The proposed solution must be able to support privilege access to both Windows joint-domain server and Windows workgroup server</p>	
<p>The proposed solution must be able to support email notification during the request- approval workflow.</p>	
<p>The proposed solution must avoid 'single point of failure or vulnerability' which will result in the catastrophic breakdown of the entire essential privileged access service to every connected target system.</p>	
<p>The proposed system must not impose any network performance constraint, in which it will act as network traffic performance choke point to degrade performance of essential privileged access to the entire target systems.</p>	
<p>The proposed web console must be viewable on common web browsers i.e., Internet Explorer, Firefox, Google Chrome.</p> <p>The proposed web console must be accessible across common desktop OS i.e., Windows XP, Vista and above</p> <p>If additional presentation capabilities are needed, should make use of one or more of the following standard plug-ins to deliver the required capability:</p> <p>HTML5</p> <p>Macromedia Shockwave 10 or above</p> <p>Flash Player 7 or above</p> <p>Adobe Acrobat Reader or above</p> <p>If a plug-in or helper application that is not listed above is required, please specify in details for justification.</p>	
<p>The proposed solution must have built-in 2FA/MFA for application login, best with One-Time-Password (OTP) method with the delivery via mobile apps, SMS, email and must support integration with third party 2FA/MFA solution.</p>	
<p>The proposed solution should provide out of box mobile apps support for authentication.</p>	
<p>The proposed solution should use proxy approach for privileged access, separating endpoints from target systems and isolating sessions to prevent the spread of malware from vulnerable end user devices to critical target systems.</p>	
<p>The proposed solution should not require additional plug-in or installer on end user devices.</p>	
<p>The proposed solution should display legal notice and disclaimer for user access.</p>	

RESTRICTED

<p>The proposed solution is able to integrate with market ready or in-house build solutions, i.e., Ticketing system, SIEM, etc.</p>	
<p>The proposed solution must have the capability to provide 100% full surveillance recording on user login via following methods:</p> <p>Console access Direct remote access from workstation Proxy remote access from multiple hops</p>	
<p>The proposed solution should provide choice to allow for comprehensive recording options across following methods:</p> <p>Host based Gateway/Proxy based Endpoint based Combination of any of the above</p>	
<p>The proposed solution should detect & record every system-based user login to the Windows and Unix target system; this should include:</p> <p>Administrator/root local console login Administrator/root remote login Every local user login Every remote user login</p>	
<p>The proposed solution should be able to record & log each user activity into respective complete user activity session file.</p>	
<p>The proposed solution must be flexible to allow user session recording in both image & text formats.</p>	
<p>The proposed solution should not use video recording which could results in high network bandwidth, large storage requirement, and unsearchable user activities events.</p>	
<p>The proposed solution should allow choice of logging & recording specifically by the following:</p> <p>-Server -User -Application launched</p>	
<p>The proposed solution should capture and display the additional information of each user session as follows:</p> <p>- User - System accessed - Login time - Logoff time - Duration - Source IP - No. of events</p>	

RESTRICTED

<p>To ease the audit & review of user session, the proposed solution should provide useful search filters such as the following:</p> <ul style="list-style-type: none"> - System - User - Event keyword (for both Input & Output) - Date - Privileged account - Session ID 	
<p>The proposed solution should allow log review capability by the following:</p> <ul style="list-style-type: none"> - Interactive user session replay - Download/Save/Print the log activities in text and image captured - Input review comment for each user session 	
<p>The proposed solution should be flexible to allow the replay of user activity in full or selectively by search & filter to achieve more effective auditing & review saving precious time. Such pin-point search capability must be powerful enough to cover even Windows's user session in GUI mode</p>	
<p>The proposed solution must possess powerful keyword search capability which shall allow one to search the recorded surveillance with keyword text -- pin point the windows GUI or text-based event with exact point in time; one can then select, play & review, then download & printout that specific action/event within the full user session for further investigation/review.</p>	
<p>The proposed solution should allow for security policy to be created & enforced diligently with policy alert setting (e.g., add new user, modify security permission in Windows.</p>	
<p>The system must be able to auto detect violation act & email alert to designated policy enforcer in real time or scheduled basis.</p>	
<p>The proposed solution should provide system process life cycle audit check to track process or service start/stop and by which user.</p>	
<p>The proposed solution should provide file & folder integrity check to ensure each change or tampering of sensitive file & folder is tracked.</p>	
<p>The proposed solution should provide the capability to monitor & track each changes/access to shared & mapped drive.</p>	
<p>The proposed solution should be able to support end point surveillance audit coverage on user activity at workstation,desktop and laptop</p>	
<p>The proposed solution must be non- intrusive to OS or kernel</p>	
<p>The proposed solution should allow applying database</p>	

RESTRICTED

<p>access control on SQLPLUS prompt i.e., block user from accessing certain sensitive table without required any changes on database permissions setting. Immediate effect upon policy published the proposed solution shall allow immediate effect upon policy published without needed the user to logoff from existing session.</p>	
<p>The proposed solution should provide privileged access via escalation of user's privilege to approved privilege within the target systems without the need to retrieve or manipulate privileged ID password (e.g., root, admin, ...)</p>	
<p>The proposed solution should provide privileged access to target system via either login through gateway (retrieve privileged password) or login to gateway then proxy auto login (with privileged ID & password) to target system</p>	
<p>The proposed solution should be able to mitigate the risk of password exposure & compromise, by providing privilege escalation in Unix/Linux & Windows platforms without retrieving, exposing or manipulating the shared privileged account password (e.g., root, administrator,) in the process.</p>	
<p>The proposed solution should allow flexible and multiple privileged levels escalation established based on origin IP(s) or access time for the same user. (e.g.: user1 with the same user ID login to server1 can be configured to have different privilege access when access comes from different IP or time more privileged access during working hours 9am to 6pm or within office LAN; restricted privileged access after working hours or via VPN)</p>	
<p>The proposed solution should provide additional facility to allow single sign on capability via gateway(s) to connect to the target system, such as: Unix, Linux, Window servers, AS400, Network devices, VMware, Database, etc</p>	
<p>The proposed solution should provide additional facility to allow proxy auto login capability via gateway(s) to connect to the target system, such as: Unix, Linux, Window servers, AS400, Network devices, VMware, Database, etc.</p> <p>Role based privilege escalation:</p> <p>The proposed solution sh support role based privilege escalation based on the custom role defined in the privilege management facility</p>	
<p>The proposed solution should enforce least privileged access at all time, every user is a normal user, until his privileged access has been escalated with independent approvals and should handle "break-glass" situation effectively</p>	
<p>The proposed solution should automatically demote or</p>	

RESTRICTED

revoke the user's privilege upon approved time expiry	
<p>The proposed solution must be able to support auto login to various target platforms via below protocols:</p> <ul style="list-style-type: none"> - SSH - Telnet - RDP - RDP Console - VNC - Web HTTP(s) - Third party client(s) 	
The proposed solution must provide an alternative option to support auto login to SSH session via native SSH clients such as PuTTY and Tectia SSH, without exposing the credential to the user.	
The proposed solution must provide an alternative option to support auto login via native file transfer clients such as WinSCP and Tectia SSH, to facilitate the file transfer function without exposing the credential to the user	
The proposed solution should provide fast & effective support of auto-login capabilities required by any new or customized enterprise application	
For gateway/proxy deployment, the proposed solution should support printing feature over RDP session, this is important especially for applications that accessed via web/client mode.	
For gateway/proxy deployment, the proposed solution should support file transfer between client & server host natively	
The proposed solution should allow configurable shared drive setting to avoid conflict of folder/drive during file transfer	
For gateway/proxy deployment, the proposed solution should support configurable secured RDP login settings such as TLS, NLA or RDP native.	
The proposed solution should provide on- screen keyboard capability for better security control.	
For gateway/proxy deployment, the proposed solution shall provide the capability to blacklist/whitelist specific command(s) during execution.	
The proposed solution should provide the capability to analyze the content (text) within the GUI.	
If a PC/server has an application that run as a foreground job and cannot be logged off, the session is locked using "cntl-alt-del lock computer" option. As a result of this, the session id had to be a common id among operators.	
The solution must have a way to identify the user/operator who is unlocking the computer for that application and log the activities done.	

RESTRICTED

The proposed solution should allow specific users to perform user management only on Active directory.	
The proposed solution should allow specific users to perform GPO administration only on Active directory.	
For Unix/Linux platform, the proposed solution must be flexible in menu configuration e.g.: server accessed from LAN network or within working hour will be prompted with local menu with additional tasks allowed but more restriction via VPN network or after working hours	
For Unix/Linux platform, the proposed solution should support SUDO like configuration from a centralized console	
The proposed solution must be able to support management of common database credentials such as Microsoft SQL Server-sa, Oracle-oradmin, etc.	
The proposed solution must be able to manage Windows service account. When a service account password reset at OS level, it must also be propagated to the relevant Windows services.	
The proposed solution must be able to supply password to the script on demand basis, so that password will not be hardcoded inside the scripts	
The proposed solution must be able to provide built-in backup in secured manner - split the privileged credentials into two files and distributed to different custodian. In the event of the password vault is not available, a process can be triggered to perform offline retrieval with the presence of the respective custodian.	
The proposed solution must be able to perform compliance check of the target systems from a centralized platform	
The proposed solution must be able to configure baseline windows password policy setting	
The proposed solution must be able to check users that are assigned with Administrators privilege in Windows Admin Account renamed check	
The proposed solution must be able to identify the "Default Administrator" account in windows system that has not be renamed --a non-compliance to the best security practice	
The proposed solution must be able to identify the Window servers that do not have the Guest account disabled which is in violation of best security practice.	
The proposed solution must be able to detect the user rights assignment has been granted to individual user directly instead of group/role on local security setting	
The proposed solution must be able to check default password, restricted password & simple password which does not comply to the password policy	
The proposed solution must be able to check disabled	

RESTRICTED

	user in Unix platform	
	The proposed solution must be able to check accounts with root UID in Unix platform	
	The proposed solution must be able to check accounts with sys UID in Unix platform The proposed solution must be able to check syslog service status in Unix platform. Dashboard view & summary report: The proposed solution should offer dash board view & summary reports, for examples as below: <ul style="list-style-type: none"> - Top 10 privileged request by user - Top 10 privileged request by Host - Top 10 password request - Top 10 result of privileged request 	
	The proposed solution must be able to list policy violation servers & the violation details	
	The proposed solution must be able to centrally check and detect dormant accounts (i.e., no login for 90 days) across Unix/Linux platforms	
	The proposed solution must be able to centrally check and list all the process/service that associated with any dormant accounts across Unix/Linux platforms	
	Bidder should quote for necessary Third-Party Licenses which are required to install their Solutions. Example: Windows License, Linux, SQL etc.	
Reporting	The proposed solution should transfer surveillance data from each target system to a centralized repository in real time	
	The proposed solution should provide comprehensive and easily customized report(s)	
	The proposed solution should allow report generation in scheduled manner like daily, weekly or monthly	
	The proposed solution must not offer vulnerable security risk with dangerous malware like key-logger for the purpose of key logging & key recording; Key-logger will record password entered via keyboard in to system, resulting to breach of privacy & security	
	The proposed solution should support report generation in PDF or CSV format.	
Security	The proposed solution should provide option to configure message to prompt user upon usage of the application i.e. All activities are subject to monitoring for compliance purpose.	
	The proposed solution shall display last successful login time & failed login attempts upon user login successfully to the system.	
	The proposed solution should prompt user to clear browser's cache & memory after logoff from the system.	
	The proposed solution should allow security officer/auditor to monitor real time and perform termination of user session upon violation detected.	

RESTRICTED

	The proposed solution should provide in-depth analysis on screenshot/image, so that text captured can be furthered indexed for better search.	
	The proposed solution should trigger email notification upon user logging off from the server.	
	The proposed solution must allow user to configure & define which user can access which user activities sessions - either by user or host	
Access Control	The proposed solution must provide host based fine grain granular access control in this configuration, none can escape the access control imposed, this includes user who bypass or circumvent proxy gateway & firewall, and any user login directly via local console mode (e.g., root & admin with local console login)	
	The proposed solution should provide easy & intuitive configuration by grouping of user or system to achieve more effective access control management	
	The proposed solution should support standard & customizable role-based access control	
	The proposed solution must be able to support Blacklist (deny specific) capability to the following: <ul style="list-style-type: none"> - Service - File/Folder - Registry - Shared folder - Command 	
	The proposed solution must be able to support Whitelist (allow specific) capability to the following: <ul style="list-style-type: none"> - Service - File/Folder - Registry - Shared folder - Command 	
	For Unix/Linux platform, the proposed solution should support menu-based access so that each user can only executes tasks defined in his/her own menu	
	The proposed solution shall enforce in- depth access control on windows services such as: <ul style="list-style-type: none"> - Deny user to start/stop but allow changing another configuration i.e., Log on As, etc. - Allow user to start/stop but block the changes of another configuration i.e., Log on As, etc 	
Password Policy	The proposed solution should provide password custody for common shared privileged account passwords of target server (e.g., root, administrator, etc)	
	The proposed solution should provide multilevel request-approval based password retrieval of common shared	

RESTRICTED

	privileged account passwords of target server (e.g., root, administrator, etc)	
	The proposed solution should provide split password custody & retrieval with dual control	
	The proposed solution must enforce password encryption in storage & in transit	
	The proposed solution must enforce scheduled periodic auto reset of privileged account passwords on the target systems	
	The proposed solution should allow manual reset of target account password reset to random value	
	The proposed solution must be able to reset target account passwords to a random value automatically upon the expiry of approved time	
	The proposed solution shall support strong and complex password policy	
	The proposed solution needs to apply AES 256-bit strong encryption or beyond Privileged account categorization: The proposed solution must be able to categories the privileged accounts via pre- defined groups	
Warranty and support	Bidder should submit BOQ of proposed device including the details part numbers, Should provide 24x7 support	
	Bidder must quote for necessary Licenses for 03 years including Technical Assistance Center support, software updates and subscription update support.	
Installation, Testing and Commissioning	Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to BANGLADESH NAVY Authority.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

b. **Active Directory Controller Software** (To be included in Server OS).

4. **Software for NOC**

a. **Monitoring Software.**

- (1) Brand : To be mentioned by bidder (Preferably Solarwind)
- (2) Model : To be Mentioned by the Bidder
- (3) Country of Origin : As per tender specification, article 20
- (4) Country of Manufacture : As per tender specification, article 20
- (5) Features:
 - (a) Multi-vendor network monitoring
 - (b) Network Insights for deeper visibility
 - (c) Intelligent maps
 - (d) NetPath and PerfStack for easy troubleshooting
 - (e) Advanced alerting
 - (f) NOC Ticketing system (Service Now)

RESTRICTED

- (g) Quantity: 200
- (h) Subscription based for 3 year
- (g) Training: Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.

b. **Vulnerability Management Software.**

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by the bidder.	
Model	To be mentioned by the bidder.	
Type	To be mentioned by the bidder.	
Country of Origin	To be mentioned by the bidder	
Country of Manufacture	To be mentioned by the bidder.	
No of Units	1	
	The Vulnerability Management solution must fully integrate vulnerability scanning and compliance audit to include combined licensing and consolidation of data, analysis, and querying.	
	The Vulnerability Management solution must include an integrated Agent and Agentless vulnerability scanning capability for full visibility of vulnerability and compliance.	
	All components of the proposed Vulnerability Management solution must be an on premise solution with minimum 1024 IP Addresses license with unlimited scanning.	
	The solution must support a variety of scan engine platforms to include Windows, Linux, UNIX/AIX, Mac OS, Network devices as well as Virtual Appliances. Please state the supported platform(s).	
	A virtual appliance must be available for scan engines and for centralized console at no additional cost, i.e., included within the licensed bundle.	
	Virtual appliance must be available for HyperV and VMware platform.	
SYSTEM DESIGN, ARCHITECTURE & PERFORMANCE	The Vulnerability Management solution must be deployed on premise and not dependent on any cloud services. The solution must support air-gapped deployment without any loss of feature and function.	
	The proposed Vulnerability Management solution must support multiple organizations within a single management console. Each organization shall have its own set of Active Scanner, User base, Asset Groups, Dashboards and Reports.	
	Active scanner within that organization can only scan asset belonging to its own organization.	
	The proposed Vulnerability Management solution must be configurable to allow for scan throttling to prevent generation of sufficient traffic to disrupt normal network infrastructure. The solution must be able fine tune scan performance by the following parameters:-	
	(a) Max Checks per Host	
	(b) Max Hosts per Scanner	
	(c) Max Scan Time	
	(d) Max TCP connections	
	The proposed Vulnerability Management solution must	

RESTRICTED

	provide the ability to support offline scanning and importing results in the server.	
	The proposed Vulnerability Management solution must allow for entry and secure storage of user credentials, including Windows local and domain accounts, and Unix su and sudo over SSH.	
	The proposed Vulnerability Management solution must provide the ability to escalate privileges on targets from normal users to root/administrative access.	
ADMINISTRATION, ACCESS CONTROL & WORKFLOW	The proposed Vulnerability Management solution must support secure web-based administration/console.	
	The proposed Vulnerability Management solution must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.	
	The proposed Vulnerability Management solution must allow administrators to:-	
	(a) limit access on a per user basis to specific asset lists, scan policies, and vulnerability repositories.	
	(b) assign resources on a per user basis such as scan policies, asset lists, queries, and credentials.	
	(c) limit scanning permissions to full scanning, scanning using specific policies, or no scanning.	
	Please state if the solution is able to support (a), (b) and (c).	
	The proposed Vulnerability Management solution must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.	
	The proposed Vulnerability Management solution must allow administrators to:-	
	(a) limit access on a per user basis to specific asset lists, scan policies, and vulnerability repositories.	
	(b) assign resources on a per user basis such as scan policies, asset lists, queries, and credentials.	
	(c) limit scanning permissions to full scanning, scanning using specific policies, or no scanning.	
	Please state if the solution is able to support (a), (b) and (c).	
	The proposed Vulnerability Management solution must provide alerting capabilities for vulnerabilities and events.	
The proposed Vulnerability Management solution must support the definition of alerts based on vulnerability scan or configuration audit results. Alert actions must include: customizable email with context specify variable, creation of a ticket, initiation of a scan, generation of a syslog event, and report generation.		
The proposed Vulnerability Management solution must have the option to support filter by AES and AES Severity		

RESTRICTED

	on vulnerabilities, dashboards, and reports	
	The proposed Vulnerability Management solution must provide Global Search capability to search for CVE-ID and host assets by IPv4	
ASSET DISCOVERY	Asset Discovery Templates should be provided by the vendor and kept up to date via a live feed. Feed update should either be online or offline.	
	The proposed Vulnerability Management solution must provide integrated:-	
	(a) web server service discovery (e.g. IIS, Apache). Please list.	
	(b) web client service discovery (e.g. Safari, Chrome, Edge, Mozilla, Opera, Tor). Please list.	
	(c) network/security device discovery (e.g. Cisco, Juniper). Please list.	
	(d) database service discovery (e.g. Oracle, IBM DB2, PostgreSQL, Mongo DB, Maria DB, MySQL, MSSQL). Please list.	
	(e) ability to identify assets based upon compliance checks – include but not limited to NIST 800-53, SCAP Systems, CIS. Please list.	
	(f) ability to discovery Virtual Technology – include but not limited to Citrix Clients and Servers and XenServers, VMware ESX Hypervisors. Please list.	
	The proposed Vulnerability Management solution must be capable of detecting the presence of a USB Device – Generic, Apple iPod, IronKey, SanDisk, USB Mass Storage.	
	The proposed Vulnerability Management solution must be capable of detecting services that are running on non-standard ports.	
	The proposed Vulnerability Management solution must be capable of detecting the following Client Applications (but not limited to) – Chrome, Firefox, Opera, Safari, Internet Explorer Web Browsers, Skype, Client P2P, IE v3/4/5/6/7/8/9/10/11, TeamSpeak Online gaming VoIP Server, Upstream mobile App, Viber Client, Vonage VoIP, WeChat Client, WhatsApp Client, Snapchat Mobile App usage, Sprint TV App, Cisco IP Communicator installed, eStara SoftPhone, Foursquare App installed, IAXClient VoIP App, iTunes Mobile iOS Device Backup, Kakao Client, Line Chat client, Mobile Chat Apps, ActiveSync clients, Client IRC, Anti-Virus Current (the remote Windows or Mac OS X host has an antivirus installed and running and it's engine and virus definitions are up to date), Clients IMAP, HTTP and FTP, Anti-Virus Outdated, Microsoft Office 2007 and 2010, Cisco Unity, IBM DB2 Client, Oracle/Microsoft SQL/Sybase SQL-Anywhere and MySQL clients.	
	Please list all the client application that can be detected.	
	The proposed Vulnerability Management solution must be	

RESTRICTED

	capable of detecting and identifying assets relating to the latest and most current vulnerabilities – Shellshock, HeartBleed (Vulnerable Systems and New SSL Certificates), Cisco VoIP Vulnerable Systems, SSH, RSH, RLOGIN, Telnet Authenticated Check for Linux.	
	The proposed Vulnerability Management solution must be capable of detecting assets based upon the following network behaviors – Hosts with Internal Connections FROM other Hosts, Hosts with Internal Connections TO other Hosts, Social Network Activity, YouTube Access, Mobile Application Activity, Voice or Mobile Client Devices, VoIP Client, VoIP Protocols, SIP, Slacker Application Music Streaming, Netflix On-Demand Media Streaming, Pandora Mobile Device Internet Radio Streaming, Cellular Phone Browser Detection, Cisco Phone Client, Hulu On-Demand Media Streaming, iPhone App Installed, iPhone Exchange Usage, Last.fm App Music Streaming, Media gateway Control Protocol (MGCP), Mobile Device Streaming Video, Android mobile Device App Download, Apple FaceTime, Apple iPhone Mail, Apple iPhone Web utility Detection, Apple iPhone Wireless Connection, Internet Browsing Systems, VPN Protocols, DHCP Clients, Snort Hosts, H.323 Protocol or VoIP Application, Windows RDP or Terminal Services.	
	The proposed Vulnerability Management solution must have the option to allow user to change the asset criticality rating determine by the system to better reflect the role of assets within its organization.	
	The proposed Vulnerability Management solution must provide the ability to discover internet-facing assets, domains and subdomains without using any agent or scanner approach.	
VULNERABILITY SCANNING	The proposed Vulnerability Management solution must be capable of both agent and agentless scanning on both local and remote vulnerability detection.	
	The proposed Vulnerability Management solution must provide a significant amount of vulnerability checks beyond the Windows operating system.	
	The proposed Vulnerability Management solution must be capable of tracking DHCP changes by associating scan results with system hostnames.	
	The proposed Vulnerability Management solution must support the ability to preserve scan results of inactive hosts for a customizable period of time Vulnerability Identification.	
	The proposed Vulnerability Management solution must detect and rank issues, risks, and vulnerabilities. It must also provide detailed information regarding the nature of the risk and recommendations to mitigate them.	
	The proposed Vulnerability Management solution must provide large of signature/fingerprint/plugin that identify	

RESTRICTED

	vulnerabilities, malware and sign of compromise.	
COMPLIANCE AUDITING	The proposed Vulnerability Management solution must be capable of agent and agentless compliance auditing	
	The proposed Vulnerability Management solution must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and vendor best practice standards. Vendor must support all the following benchmarks:	
	PCIDSS, CERT, CIS, BSI, DISA STIG, NSA, NIST, Microsoft SCM.	
	The proposed Vulnerability Management solution must provide vulnerability auditing of Operating Systems, Routers, Switches, network devices and Applications.	
	The proposed Vulnerability Management solution must provide security and configuration auditing benchmarks for vendor best practices such as Microsoft, Cisco, and Vmware etc.. List the best practice benchmarks supported.	
	The proposed Vulnerability Management solution must provide auditing of Microsoft operating systems for security and configurations settings. List the versions supported with available benchmarks.	
	The proposed Vulnerability Management solution must provide auditing of all major Unix operating systems for security and configurations settings. List the operating system vendors and versions supported with available benchmarks.	
	The proposed Vulnerability Management solution must allow audit policies to be customizable for organizational specific needs.	
	The proposed Vulnerability Management solution must provide Center for Internet Security (CIS) Certified Benchmarks for Compliance and Audit Policies. CIS Audit Policies should be available for the following Operating Systems and Applications:	
	IBM AIX, Apache, Apache Tomcat, BIND, CentOS, Debian Linux, FreeBSD, HP-UX, RHEL, Solaris 10 and 11, SuSE SLES, Ubuntu, Microsoft Internet Explorer 9 and 10, Microsoft Exchange Server 2007, Microsoft IIS, Microsoft Office Windows 2000, Windows Server 2003, Windows XP, Windows Server 2008, Windows 7, Windows Server 2012, Windows Server 2016, 2019, 2022, Mac OS X Leopard and Snow Leopard	
The proposed Vulnerability Management solution must be NIST Security Content Automation Protocol SCAP Validated - a set of policies for managing vulnerabilities and compliance.		
REPORTING	The proposed Vulnerability Management solution must support the generation of fully customized reports directly from the management console using either vendor	

RESTRICTED

	supplied templates or without templates.	
	There should be a large number of vendor supplied templates for reporting. New templates must be automatically downloaded to the management console. (Please list the number of reporting templates provided).	
	The proposed Vulnerability Management solution must provide the ability to filter results in reporting by a variety of criteria to include asset lists, repositories, addresses, vulnerability types, raw text, and date fields.	
	The proposed Vulnerability Management solution must provide integrated reporting of active scanning.	
	The proposed Vulnerability Management solution must provide the ability the fully automate reporting to include scheduled report execution and delivery and post-scan report delivery.	
	The proposed Vulnerability Management solution must provide the ability to produce ad hoc reports while viewing results in the console. PDF and CSV exports shall be available.	
	The proposed Vulnerability Management solution must support the ability to produce reports in the following report formats: PDF, CSV, XML	
	The proposed Vulnerability Management solution must provide pre-configured Report Templates for the following categories:	
	Advanced Persistent Threats & Malicious Software, Botnets, Centre for Internet Security, Configuration & Patch Auditing, Exploits & Attack Paths, Logging, Monitoring & Intrusion Detection, Mobile Devices, USB Devices & Wireless, Scan Monitoring, Patch Deployment, Payment Card Industry, SANS, Vulnerability Reporting, Web Application Security	
	The proposed Vulnerability Management solution must include Predictive Prioritization that analysis the detected vulnerability with threat data using advanced data science algorithm. Each vulnerability should have a rating that incorporates the result of this analysis. This rating should be updated on a daily basis to reflect the actual threat landscape.	
Integration	The proposed Vulnerability Management solution must have integration capability with 3rd Party Penetration tool like Metasploit Pro, Core Impact etc.	
Implementation	Professional Implementation service must carry out on site installation, testing and commissioning.	
Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, software updates and subscription update support one (1) years.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	

c. **Active Directory (AD) Security.**

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by bidder (Preferably Tenable)	
Model	To be mentioned by the bidder.	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Technical General Requirement	Please state the principle/vendor and product/solution name of the proposed Active Directory (AD) Security solution.	
	The proposed solution block threats in real time as soon as lateral movement is detected across both the authentication layer or endpoints to improve response times dramatically and eliminate the need to hunt through logs.	
	The Solution should provide unified platform for endpoint and identity security with a single agent and console for immediate time-to-value.	
	The Proposed solution must stop attacks from endpoint to cloud with complete visibility across traditional Active Directory (AD), empowered with industry-leading threat intelligence.	
	The Proposed solution should find stealthy attacks with AI-powered detection.	
	The proposed solution should continuously monitor user behavior and risk context with dynamic enforcement of multi-factor authentication (MFA) when risk changes. Seamlessly extend MFA coverage to legacy systems and protocols that are likely to be exploited.	
	With the proposed solution, user should be able to see full attack paths and correlate threats within a single console.	
	The solution should result in faster responses and real-time protection, offsetting thousands of hours of post-breach investigation every year.	
	The solution should have capabilities to provide deep visibility into compromised passwords, over-privileged accounts and service account misuses.	
	The solution should have to enables to proactively address Active Directory hygiene issues and establish proactive controls, thereby reducing compliance costs	
	The solution should have to have ability to detect identity specific threats allowing users to identify high-risk accounts and possible attack paths across their entire environment, reducing the attack surface.	
The proposed solution to provide granular visibility over		

RESTRICTED

	incidents involving protocols like NTLM, Kerberos, SMB and LDAP/S, which are impossible or difficult to detect with traditional tools like next-generation firewalls, and user and entity behavior analytics (UEBA)	
	The installations should take very less time to see all identities on the network and start identifying anomalies immediately.	
	The proposed solution should have behaviour based indicators and profiling where profiles are based on both static information from identity stores and dynamic information in real time to catch insider threats, lateral movement and privilege or service account abuse. Eliminate risk guesswork and prioritize authentication tasks based on over 100 behavior analytics and risk scores for every account.	
	The solution should detect identity store threats (and typical red-team exercise tests) like NTLM/LDAPS protocol threats, Golden Ticket attacks, Pass-the-Hash and other credential theft, as well as persistence techniques. Safely lure adversaries away from high-value resources and gain dedicated insights into their attack paths.	
	The solution should have internal Threat Hunter feature to offer visibility for all credential attacks and incident response, showing the chain of activity and subsequent increase in risk score.	
	The administrator should be able to export in common event format (CEF) or Log Event Extended Format (LEEF) to any SIEM or to SOAR tools via API.	
	The solution should discover all identities across the enterprise, including stale accounts, with password hygiene	
	The solution should have capability to improve alert fidelity and reduce noise by recognizing true positive events of interest.	
	The solution should detect anomalous activity without requiring logs.	
	The proposed solution should offer threat detection, a low false positive rate and the ability to detect threats that are difficult to detect via post-event, log-based security tools.	
	The proposed solution should works for identity stores on-premises or in the cloud, and for users/applications anywhere without any agents on endpoints or servers outside the domain controllers.	
	The solution should extend identity verification/MFA tools to any resource or application, including legacy/proprietary systems and legacy systems traditionally not integrated with MFA — such as desktops, tools like PowerShell and protocols like RDP	

RESTRICTED

	over NTLM — to reduce the attack surface.	
	The solution should designate accounts as honeytokens to safely lure adversaries away from your critical resources, with dedicated insights into their attack paths.	
	The solution should detect the following attacks:	
	-DCShadow	
	-DCSync	
	-Golden Ticket	
	-LSASS Memory Injection	
	-Kerberoast attack	
	-NTDS Extraction	
Implementation	Professional Implementation service must carry out on site installation, testing and commissioning.	
Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, software updates and subscription update support one (1) years.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

c. **Penetration Testing Solution.**

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned by bidder (Preferably Tenable)	
Model	To be mentioned by the bidder.	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Technical Requirement	General Requirement	
	Please state the principle/vendor and product/solution name of the proposed Penetration Testing solution. Please list down all the software components of the PT solution.	
	Installation, Deployment and Integration	
	Solution must be deployed on premise and able to support installation on 64-bit Linux and Windows (64-bit) Virtual Platform or Bare Metal server.	
	Solution shall have latest updates (e.g. exploit module) as frequent as on a weekly basis.	
	Solution shall support offline activation and manual updates.	
	Solution must be able to perform full backup to prevent data loss and enable to easily migrate data.	
	Administration	
Solution shall allow API integration with other systems or		

RESTRICTED

	be able to automate workflow.	
	Solution must be able to run jobs or tasks (e.g. scan, exploit) on schedule.	
	Host Scan and Web Scan	
	Solution shall support dry runs to show the scan information in task log only.	
	Solution must be able to integrate with Nexpose to discover host's OS, running services and vulnerabilities via existing scan results or new scans.	
	Solution must support importing of scan result from external solutions including but not limited to Nexpose, Metasploit, Foundstone, Microsoft, nCircle, NetSparker, Nessus, Qualys, Burp, Acunetix, AppScan, Nmap, Retina, Amap, Critical Watch, IP Address List, Libpcap, Spiceworks and Core Impact.	
	System Exploitation	
	Solution shall automatically select and apply exploit modules based on OS, service and vulnerability references.	
	Solution shall have at least 6 reliability levels of exploit codes for automated exploitation.	
	Solution shall support running individual exploit module manually from the user interface.	
	Solution shall support dry run to show exploit information in task log only.	
	Solution shall support replay of exploitation tasks.	
	Solution shall support the reuse of manually added or captured credentials within a project to validate specified credentials on additional hosts in the target network.	
	Bruteforcing	
	Solution shall support bruteforce testing on services including but not limited to AFP, SMB, Postgres, DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, SSH PUBKEY, Telnet, FTP, POP3, VNC, SNMP, WinRM.	
	Solution shall support customized credentials and dictionary import for bruteforce.	
	Solution shall support credential mutation to create multiple permutations of a specified password, which enables building of a larger list based on a defined set of passwords.	
	Post Exploitation Action And Evidence Collection	
	Solution must support exploitation payload types "Meterpreter", "Command Shell" and "Powershell" etc.	
	Solution must support customized macros to run selected operations automatically after exploit.	
	Solution must support post exploitation actions including but not limited to collect system data (screen capture, password, system information), build a virtual desktop connection, access file system, search the file system, run a command shell, create proxy pivot, create VPN pivot.	

RESTRICTED

	Solution must support deploying of persistent listeners to allow exploited hosts to connect back to Metasploit automatically.	
	Social Engineering Campaign	
	Solution must support web campaign, Email campaign and USB campaign.	
	Solution must allow web campaign customized with http/https, IP address, port and path (e.g. https://www.abc.com:1234/abcd).	
	Solution must support web content to be cloned from another web site (e.g. www.google.com).	
	Solution must support web campaign that browser autopwn (apply all the appropriate exploit modules based on the browser version), specific browser exploit (e.g. MS11-050) and not do anything (just checking the connection from the users).	
	Solution must support email campaign content customization to include a specific URL or an agent attachment.	
	Solution must support USB campaign that generates an agent deployment .exe file.	
	Report and Data Export	
	Solution must provide built-in standard reports and support customized report functionality.	
	Solution must support reports to be stored locally and sent to recipient by email after created.	
	Solution must be able to support data export which allows a zip archive of the project suitable for importing into an another instance of the solution.	
Implementation	Professional Implementation service must carry out on site installation, testing and commissioning.	
Support Warranty with License Requirements	Support bundle including parts & labour with 24x7x365 days OEM support, software updates and subscription update support one (1) years.	
	Bidder should submit detail BoQ mentioning the OEM part numbers.	
	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

d. Server Security Solution, (Subscription: 01 years)

Specifications	Description of Requirements	Bidder's Response
Brand	To be mentioned by bidder (Preferably Trend Micro)	
Model	To be mentioned by bidder	
Country Of Origin	As per tender specification Article no 20	
Country of Manufacture	As per tender specification Article no 20	

RESTRICTED

Type	On premises	
Solution functionality and supported features	The solution must provide single platform for complete server protection over physical, virtual (server/desktop)	
	Provides layered defense against advanced attacks and shields against known exploitable vulnerabilities in web and enterprise applications and operating systems.	
	Web reputation prevents access to malicious web sites	
	Protects a wide range of OS on different platforms: Windows, Linux, Solaris, AIX on VMware, Citrix, Hyper-V, Amazon etc.	
	The proposed solution provides self-defending servers; with multiple integrated modules below providing a line of defense at the server: firewall, Anti-Malware ,HIPS, Integrity Monitoring, Application Control etc.	
	Proposed solution must have a web based dashboard which should be configurable by administrator to display the informations which are required only.	
	Providing "Alerts" on the main menu to view administrator notifications concerning system or security events.	
	Providing Firewall Events to view activities on computers with the firewall enabled (typically includes dropped or logged packets).	
	Providing access to DPI Events to view security-related DPI activities. The section should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode).	
	Providing System Events to view a summary of security-related events, primarily for the Management server and also including Agents' system events. All administrative actions should be audited within the System Events.	
	Must be able to avoid resource contention such as antivirus Strom in the virtualised VDI environment.	
	The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites for virtual desktops	
	The proposed solution should provide agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware etc.	
	The proposed solution should have Machine learning technologies which can perform in-depth file analysis to detect emerging security risks through digital DNA fingerprinting, API mapping, and other file features.	
	Must be able to provide HIPS/HIDS feature with agent in Physical & virtual servers.	
	Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.	
Must be able to operate in detection or prevention mode		

RESTRICTED

	to protect operating systems and enterprise application vulnerabilities.	
	Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred	
	Must be able to provide protection/shield against known exploitable vulnerabilities.	
	Protection can be pushed out to thousands of virtual/physical servers in minutes without a system reboot.	
	Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services	
	Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits	
	Must assist compliance (PCI DSS) to protect web applications and the data they process.	
	Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.	
	Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.	
	The proposed solution should be capable enough to integrate with on-premises Sandbox appliance of the same vendor. (Sandbox should be procured separately).	
	Fine-grained filtering (IP and MAC addresses, ports).	
	Coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)	
	The proposed solution should have basic prevention of denial of service (DoS) attack from day one.	
	Design policies per network interface.	
	Detection of reconnaissance scans.	
	Must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in Windows, Linux, AIX & Solaris systems.	
	The proposed solution should scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services.	
	Provide virtual protection which shields known remotely exploitable vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.	
	Must have vulnerability rules to shield known remotely	

RESTRICTED

exploitable vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours.	
The proposed solution should be able to find important events (Detect suspicious behavior, error and informational events like disk full, service start, service shutdown, etc.) from operating system and application logs.	
The Tag must be fully customizable; Administrator can add, edit and delete their own Tag with own name	
The solution should support Application control, behavior monitoring & Ransomware protection.	
The solution should support on premises Anti-APT solution integration.	
The solution should have anti-malware scanning capacity in Oracle Solaris 10 & 11	
Support Platform:	
Microsoft Windows -	
• Windows 7, 8, 10	
• Windows 2008 (32 and 64 bit) server	
• Windows 2012, 2016,2019, 2022 server	
Virtual platform supported -	
• Vmware vSphere 4.1/5.0/5.1	
• Vmware ESXi 5.0/5.1	
• Vmware View 4.5/5.0	
• Citrix XenServer	
• Microsoft HyperV	
Solaris -	
• Solaris OS 10	
• Solaris OS 11	
Linux -	
• RedHat Enterprise Linux 6.0, 7.0, 8.0, 9.0	
• SUSE Enterprise Linux 8 (32-bit/64-bit)	
• SUSE Enterprise Linux 10 (32-bit/64-bit)	
Unix -	
• AIX 5.3,6.1 on IBM Power Systems	
Ubuntu 22,20,18,16,14,10	
Compliance & Certification:	
Provides out of the box compliance support for	
PCI DSS 2.0.	
NIST	
HIPAA	
SOX	
ISO 2700x	
The solution must be certified to Common Criteria EAL 2+.	
Deployment and Integration:	
The solution must be integrated to SIEM system including ArcSight™, Intellitactics, NetIQ, RSA Envision, Q1Labs, Loglogic.	

RESTRICTED

	Directory integration so that it integrates with enterprise directories, including Microsoft Active Directory	
	Must be able to integradable to vSphere, vCenter, vCloud seamlessly.	
	Software distribution, with agent software that can be deployed easily through standard software distribution mechanisms such as Microsoft® SMS, Novel Zenworks, and Altiris.	
Third Party Licenses	Bidder should quote for necessary Third-Party Licenses which are required to install their Solutions. Example: Windows Std Server License , Microsoft SQL Std server License etc.	
Warranty and support	Bidder should submit BOQ of proposed Solution including the details' part numbers	
	Bidder must quote for necessary licenses for 03 years including Technical Assistance Center support, software updates and subscription update support.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

e. DNS Firewall with DHCP and IPAM (Subscription: 1 years)

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned By the bidder. (Preferably EfficientIP)	
Model	To be mentioned by the bidder.	
Country of Origin	As per tender specification Article no 20	
Country of Manufacture	As per tender specification Article no 20	
General Requirement	DNS System must be an Hardware Appliance based solution providing with defined features & capacity from single OEM.	
	DNS System must provide integrated support for high availability configurations without the requirement for licensing of additional third -software components.	
	DNS System must support System logs forwarding/redirection of logs to a defined syslog host.	
	DNS system must support monitoring using SNMPv3	
	DNS system must support NTP time synchronization (client-mode) to multiple servers.	
	DNS system must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory	
	DNS Solution must support GUI & CLI based configuration.	
DNS Specific Requirements (Cache &	The Solution must support 50,000 DNS QPS Day1 & should be scalable upto 200,000 DNS QPS DNS Server in future through additional software license on	

RESTRICTED

Recursive DNS Server)	the same proposed DNS Hardware Appliance.	
	System should have a Cache & Recursive DNS Server	
	System proposed should be deployed 2 Qty at DC & 2 Qty at DR as as dedicated Cache & Recursive DNS Server.	
	System should have a Cache DNS Architecture to switch on demand from BIND to UNBOUND and vice versa on same system.	
	System should be able to support the following common resource record types namely A, AAAA, DNAME, CNAME, MX, HINFO, PTR, SOA, NX	
	System should be deployed on-premise & should not be an Cloud based solution.	
	System should regularly monitor its cache contents and automatically purge / remove records that are old	
	System should have a built-in RPZ functionality and does not require additional licences to enable such feature	
	System RPZ should support action as Block, walled redirection, no response	
	System should support Access Control based on Source IP for Allow Query, Allow Query Cache.	
	System should Support DNSSEC	
	System must support Anycast for DNS with BGP, IS-IS and OSPF	
	System should support audit log.	
	System should support granular rights administration limiting the function and rights to user and record level	
	System should support sending logs to external Syslog server	
	The Solution should have the ability to Log Only, Block & Quarantine poorly behaving clients based on their DNS Transactions.	
	The Solution should provide for DNS Cache Saving to retain Cache Data even while applying software updates, patches, upgrades and reboot.	
	The Solution should have the ability to identify the poorly behaving clients based on their DNS Transactions & only allow client to access DNS Cache entries.	
	The Solution should have the ability to identify the poorly behaving clients based to allow clients to access Cache & restrict recursive query which seems to exfiltrate the using DNS protocol.	
	The solution must be both IPv4 and IPv6 compatible.	
	The Caching DNS Solution should be able to identify clients using any of the below identifiers to be used as	
	DNS Access Control List	
	DNSMASQ Mac Address	
EDNS Client Subnet		
Nominum CPE and Device ID		

RESTRICTED

OpenDNS Device and IP	
System should be able to instantly mitigate multiple DNS threat vectors such as	
DNS tunnelling	
Volumetric NXDomain DoS attacks	
Phantom domain attacks	
BIND Zero day vulnerability attacks	
DNS cache poisoning attacks	
DNS Amplification and Reflection Attacks	
Resource Utilization Attacks	
DNS hijacking	
Domain lock-up attacks	
Basic NXDOMAIN attack	
Random subdomain attack	
DNS Sloth Attack	
Recursive layer attack	
The proposed OEM should have an in-house threat research team to provide real-time intelligence and depend on third-party feeds to enrich the threat feeds.	
The proposed OEM must have his own Threat Intelligence unit.	
Threat Intel feeds with the following categories or equivalent :	
a. Malware	
b. Botnet	
c. DGA	
i. Time Dependent	
ii. Non Time Dependent	
d. Abuse	
e. Phishing	
f. Miner	
g. Suspicious	
h. Newly Observer Domain with following timelines	
i. 1 Day	
ii. 7 Days	
iii. 30 Days	
The Proposed OEM should provide their Threat portal access to find below characteristics of any internet registered domain:	
i. Threat Category (if domains is already known malicious domain)	
ii. Risk score ranging from A (low risk) to F (high risk)	
iii. Host server IP address and country for a given Domain Name	
iv. Presence in Threat Intelligence sources	
v. Whois & SSL certificate information	
vi. Other DNS and web information that should provide history of DNS records associated with a FQDN, other FQDNs associated with the same IP address, word map, website screenshot.	

RESTRICTED

DNS Specific Requirements (Internal Authoritative DNS Server)	Solution should support standards-based DNS services.	
	The solution should support the ability to act as an internal Authoritative nameserver & should be an Hardware Appliance.	
	The Solution should support 50,000 DNS QPS acting as Internal Authoritative DNS Server	
	The Solution Should support to configure 100 Zone.	
	The Solution Should support to configure 20000 record	
	The Solution shoul support Master-Slave, Multi Master or Stealth Mode deployment architecture.	
	The solution should be able to automate common tasks such as maintaining synchronization between forward and reverse records	
	Authoritative Name Servers should have the built-in protection using Response Rate limiting	
	The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)	
	The Solution should support A, NAPTR, SRV, NS, MX, CNAME records	
	Should support IPv6 : AAAA, PTR, host, ip6.arpa, DDNS records	
	Solution should support multiple DNS views based on IPv4/Ipv6 Addresses	
	The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc	
	The solution should support easy search, sort and filter on any DNS Zone or RR, using any field	
	Theproposed solution must support the ability to control DNS logging : DNS query and response logging	
	The solution should provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.	
	The system should be able to display all hosted DNS Resource Records in one GUI pane	
	Import Wizard solution must be built-in solution by the DNS Appliance and must not require any external Java program or external Virtual Machines	
	The solution should provide a means to track changes to made via Dynamic DNS record assignment	
	The solution must support the standard DNSSEC specifications for serving of DNSSEC signed zones and the passthrough of client resolution of external zones	
The solution must support secure dynamic updates from Microsoft clients using the Microsoft Generic Security Service Transaction Signature (GSS-TSIG) standard		

RESTRICTED

	The solution must support TSIG for authentication of zone transfers and dynamic updates	
	The solution must have inbuild reports & Stats.	
	System proposed should be deployed 2 Qty at DC & 2 Qty at DR as as dedicated Internal Authoritative DNS Server	
DNS Specific Requirements (External Public Authoritative DNS Server)	Solution must support standards-based DNS services.	
	The solution must support the ability to act as an External Authoritative name server & proposed should be an Hardware Appliance.	
	The Solution must support 50,000 DNS QPS acting as external Authoritative DNS Server.	
	System proposed should be deployed 2 Qty at DC & 2 Qty at DR as dedicated External Authoritative DNS Server.	
	External Authoritative DNS Server must be deployed in Hidden Master Architecture with Hidden Master server placed at both DC & DR.	
	The Solution must support to configure 1000 Zone & 50000 Records.	
	The Solution must support Master-Slave, Multi Master or Stealth Mode deployment architecture.	
	The solution must be able to automate common tasks such as maintaining synchronization between forward and reverse records	
	Authoritative Name Servers must have the built-in protection using Response Rate limiting	
	Authoritative Name Servers must have the built-in protection using DNS DDoS protection - DNS Amplification/DNS reflection attacks.	
	The Solution must support A, NAPTR, SRV, NS, MX, CNAME records	
	The Solution must support IPv6: AAAA, PTR, host, ip6.arpa, DDNS records	
	The Solution must support multiple DNS views based on IPv4/Ipv6 Addresses	
	The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.	
	The solution must support easy search, sort and filter on any DNS Zone or RR, using any field	
	The product must support the ability to control DNS logging: DNS query and response logging	
	The solution must provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.	
	The system must be able to display all hosted DNS Resource Records in one GUI pane	
	The solution must provide a means to track changes to made via Dynamic DNS record assignment	
	The solution must support the standard DNSSEC	

RESTRICTED

	specifications for serving of DNSSEC signed zones and the pass through of client resolution of external zones	
	The solution must have inbuilt reports & Stats.	
IPAM	The IPAM Solution must support 20000 IP Address Management for both IPv4 & IPv6 together & should be scalable to 100000 IP address in future through additional license on the same proposed IPAM Hardware Appliance.	
	The solution must NOT use software agents or thick clients	
	The IPAM solution must provide high-availability at DC	
	System proposed should be deployed 1 Qty at DC & 1 Qty at DR as dedicated IPAM Server.	
	The solution should provide appropriate automated failover without any manual intervention.	
	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.	
	The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.	
	The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records	
	The IPAM solution should be able act as Central management Server for proposed DNS & DHCP Server from single vendor & should have inbuilt reporting for IPAM Appliance for proposed DDI Solution.	
	The IPAM solution should be able to create its own widget to display customized subnet reports, free IP, used IP.	
	The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network.	
	DDI IPAM user interface must be web-based without specific browser vendor requirements	
	DDI IPAM system should support Auto seamless failover within DC	
	DDI IPAM system should support VLSM (Variable Length Subnet Masks)	
	DDI IPAM system should be able to export reports in PDF, CSV format	
	DDI IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability.	
	DDI audit records should contain a timestamp, username and record modified.	

RESTRICTED

	DDI Reporting engine should include audit reports.	
	DDI system should support granular rights administration limiting the function and rights to user and Subnet level	
	The tool must have the capability to find free address space across a range	
	The IPAM Solution component must perform host discovery using a variety of methods not limited to ping, Address Resolution Protocol (ARP) via SNMP protocol to 3000 number of L3 Switches & Routers.	
	IPAM solution must perform host discovery using a variety of methods including SNMP, ICMP	
	The IPAM Solution Component must discovery 2000 Cloud Instances running on Amazon AWS, Google GCP & Microsoft Azure and Virtual Instance running on Vmware Vcenter	
DHCP	The solution must provide an easy to use "import wizard" to import DHCP records from legacy DHCP Solution	
	Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines	
	System proposed should be deployed in HA of 1 Qty at DC & 1 Qty at DR as dedicated DHCP Servers	
	The DHCP solution must provide high-availability	
	The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making the change, and a timestamp. The solution should also be able to identify the client IP address from where the change was made.	
	The solution must be able to handle 2000 DHCP Lease/sec & should be scalable to handle 5000 DHCP Lease/Sec in future through additional license on the same proposed Hardware Appliance without any change in Hardware appliance.	
	The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.	
	The solution must graph (visually display) the different scopes based on number of IP's used/available over a set period of time	
	The DHCP solution must support one IP per MAC address (one lease per client).	
	The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP	
	The solution must provide device finger printing and display or report the data in the GUI	
	The solution must support creating DHCP custom options.	
	The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc	
The DHCP Solution must integrate to IPAM for lease		

RESTRICTED

	consolidation and capacity planning	
	The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses	
	The DHCP Solution must be able to send alerts in case of DHCP related attacks	
	The DHCP Solution must have inbuilt Reports & stats.	
Warranty and support	Bidder should submit BOQ of proposed device including the details part numbers, Should provide 24x7 support	
	Bidder must quote for necessary Licenses for 01 years including Technical Assistance Center support, software updates and subscription update support.	
Installation, Testing and Commissioning	Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to BANGLADESH NAVY Authority.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

7. **End User Software.**

a. **Windows OS for End User PC (To be included with PC).**

- (1) Brand : Windows
- (2) Version : 11 Enterprise Edition
- (3) User : Device License
- (4) License Type: Perpetual
- (5) Bitlocker : To be included with the license

b. **Linux OS for NOC and SOC PC.**

- (1) Brand : Linux (Ubuntu)
- (2) Version : Latest version
- (3) User : Single User
- (4) Subscription : 03 years

c. **End User- End Point Protection (Antivirus and Anti Malware)
(Subscription : 1 years)**

Feature List	Feature Description	Bidder's Response
Brand	To be mentioned By the bidder. (Preferably Trend Micro)	
Model	To be mentioned by the bidder.	
Country of Origin	As per tender specification Article no 20	
Country of Manufacture	As per tender specification Article no 20	
Type	On premises	
Solution functionality and supported features	Must offer comprehensive client/server security by protecting enterprise networks from which includes virus protection, spyware, rootkits, bots, gray ware, adware, malware and other computer bourne threats or mixed threat attacks or any emerging cyber attacks or zero day attack protection. The solution should be in the of Gartner's leader's quadrant for Endpoint for last 3 years.	
	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.	
	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
	Must include capabilities for detecting and removing rootkits	
	Must provide Real-time spyware/gray ware scanning for file system to prevent or stop spyware execution	
	Must have capabilities to restore spyware/grayware if the spyware/grayware is deemed safe	
	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take	

RESTRICTED

	action based on the evaluation	
	Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process	
	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to :	
	a) Terminating all known virus processes and threads in memory	
	b) Repairing the registry	
	c) Deleting any drop files created by viruses	
	d) Removing any Microsoft Windows services created by viruses	
	e) Restoring all files damaged by viruses	
	f) Includes Cleanup for Spyware, Adware etc	
	Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether	
	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak	
	Behavior Monitoring :	
	a) Must have behavior monitoring to restrict system behavior, keeping security related processes always up and running	
	b) Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	
	Must provide Real-time lock down of client configuration allow or prevent users from changing settings or unloading/uninstalling the software	
	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
	CPU/memory(physical or virtual) usage performance control during scanning :	
	a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer	
	b) Adjusts the scanning speed if:	
	b.1) The CPU usage level is Medium or Low	
	b.2) Actual CPU consumption exceeds a certain threshold	
	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	
	Should have Integrated spyware protection and cleanup	
	Should have the capability to assign a client the privilege to act as a update/master relay agent for rest of the	

RESTRICTED

	agents in the network	
	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
	shall be able to scan only those file types which are potential virus carriers (based on true file type)	
	Should be able to detect files packed using real-time compression algorithms as executable files.	
	shall be able to scan Object Linking and Embedding (OLE) File	
	Must provide Web threat protection by the following ways:	
	a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings	
	b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location	
	c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies	
	d) Must provide real-time protection by referencing online database with millions of rated Web domains	
	e) Configure Web reputation policies and assign them to individual, several, or all end users machine.	
	Must provide File reputation service	
	a) Must be able to check the reputation of the files hosted in the internet	
	b) Must be able check the reputation of the files in webmail attachments	
	c) Must be able to check the reputation of files residing in the computer	
	Must protect clients and servers on the network, high performance network virus scanning, and elimination.	
	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	
	Must have smart feedback to enable feedback from the client agents to the threat research centers of the vendor.	
	Uses any alternate method other than the conventional pattern based scanning with the following features:	
	a) Provides fast, real-time security status lookup capabilities in the cloud	
	b) Reduces the overall time it takes to deliver protection against emerging threats	
	c) Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints	
	d) Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	
	Should be able to deploy the Client software using the following mechanisms:	
	a) Client installation Package (Executable & Microsoft	

RESTRICTED

	Installer (MSI) Package Format), should support silent installer, unmanaged clients, specific installer for servers	
	b) Web install page	
	c) Login Script Setup	
	d) Remote installation	
	e) From a client disk image	
	Must provide a secure Web-based management console to give administrators transparent access to all clients on the network	
	The management server should be able to download updates from different source if required.	
	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.	
	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	
	Should have role based administration with active directory integration	
	a) To create custom role type	
	b) To add users to a predefined role or to a custom role	
	Should have integration with the Active directory 2008/2012 or higher	
	Shall support grouping of clients into domains for easier administration.	
	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	
	Must be capable of uninstalling and replacing existing client antivirus software and to ensure unavailability of any residual part of the software.	
	Must support plug-in modules designed to add new security features without having to redeploy the entire solution, thereby reducing effort and time needed to deploy new security capabilities to clients and servers across the network.E.g. Mobile Security, etc.	
	Security Compliance should leverage Microsoft Active Directory services to determine the security status of the computers in the network	
	The solution should support client installation on all the following:	
	a) Window 8, Windows 10 (32-bit version & 64-bit version) and higher version if any	
	b) Microsoft Cluster Server having all applicable versions	
	c) Microsoft Windows Server 2008/2012 with all its versions	
	d) Client/solution installation on operating systems hosted on virtualization environment.	
	e) Should support Intel x64 , AMD x64 , any other variants of processor.	
	f) Must be able to send notifications whenever it detects a security risk on any client or during a security risk	

RESTRICTED

	outbreak, via E-mail, SMS, SNMP trap.	
	Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from client IPS, cliert firewall, and/or network virus logs exceed certain thresholds, Signaling a possible attack.	
	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack.	
	Should perform Boot & Rootkit scan and cleaning	
	AV should be seamleasssly implemented on all the varients of Windows endpoints including Windows XP.	
	System should be configured in such a way that at no case no endpoints/remote agents will be able to commuicate with OEM cloud for obtaining updates through internet.	
	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine.	
	The solution should have latest machine learning technology in built from day one.	
	The End point AV should have the option of integration with on premises sandbox/anti-apt appliance.	
	The solution should have the option of the endpoint known remotely exploitable vulnerability shiealding in the network.	
	The solution should have ransomware protection in built.	
Endpoint Detection and Response (EDR) Features	The proposed solution must have EDR capability that allows monitoring, recording, and performing of both current and historical security investigations and should help in assessing the extent of damage.	
	The proposed solution should allow users the ability to drill down on an interactive process tree that illustrates the full chain of attack in order to identify how the detection was able to arrive, what changes were made, and how it was spread by analyzing activities performed by objects and processes.	
	The proposed solution must have the ability to provide immediate response in order to terminate processes or isolate endpoint or update security and also have the ability to use current findings to sweep more endpoints.	
	The proposed solution must allow users to sweep endpoints with multiple search parameters. Sweeping must be available on parameters such as, communication being done, file hashes, registry based activity, user activity, and running processes. The proposed solution must also support industry standard Open IOC or YARA rules.	
	The proposed solution with EDR capability, a detailed root cause investigations can be made on each endpoint	
Third Party Licenses	Bidder should quote for necessary Third-Party Licenses which are required to install their Solutions. Example:	

RESTRICTED

	Windows Std Server License , Microsoft SQL Std server License etc.	
Warranty and support	Bidder should submit BOQ of proposed solution including the details' part numbers	
	Bidder must quote for necessary Licenses for 03 years including Technical Assistance Center support, software updates and subscription update support.	
Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate required policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to Bangladesh Navy Authority .	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

b. LB/WAF/DDos Management Software

Items	Required Technical Specifications	Bidder's Response
Brand	Internationally reputed Brand, bidder should mention	
Model	To be mentioned by the bidder	
Country of origin	As per tender specification, article 20	
Country of Manufacturing	As per tender specification, article 20	
CM Solution Architecture Requirement	The proposed solution have to perform as a Virtual Centralized Management provides a unified point of visibility and control for your entire portfolio, ensuring your finger remains on the pulse of devices instances, modules, and licenses and enabling you to deliver optimal application availability, performance, and security. Solution should supports instances, Modules, including hardware and Virtual appliances platform. Centralized Management system should manages policies, SSL certificates, images, and configurations for all appliances.	
	The proposed solution must support manage day to day operations from single console for proposed Load Balancer, WAF, Anti-DDoS, DNS Security & GSLB Solution	
	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot or on device packet captures on appliance config and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link.	
CM resource requirement	Central Management should support VM resource provision minium of 8vCPU, 16 GB RAM and 500GB	

	Storage or higher.	
	Data collector nodes should support VM resource provision minimum of 8vCPU and 16GB RAM and 1TB Storage or higher.	
Dashboard, Configuration, Visibility Reporting & Centralized management	The entire solution must be manageable from a dedicated central management system to centrally manage WAF, DNS, GSLB policies for day to day operations from single console.	
	Proposed central management system should provide a comprehensive overview of Load Balance, WAF, Application Access Management, Anti-DDoS and DNS traffic, services, errors, attacks, and GSLB metrics.	
	Proposed central management system should support automation like manage application with the AS3, Certificate and key management, device management, security & access management, security administration, reporting, load balancer and DNS management.	
	Proposed central management system should provide role based access control, centralized analytics logs, dashboard, auditing and across devices, services, and the applications.	
	Proposed central management system should have L7 Security Dashboard which enables users to drill into important security events and metrics such as WAF status, malicious traffic volume, web exploits, L7 DDoS attacks, bot traffic, and more.	
	Proposed central management system should have highly customizable dashboards that can: <ul style="list-style-type: none"> • Show a high-level “at-a-glance” status and analytics • Provide deep application- and role-specific views of app health and performance • Offer insights into security status, server-side round trip time, specific browser performance, and many other helpful metrics • Extend visibility, analytics, and basic configuration controls to legacy app services 	
	The proposed solution should provide a catalog of application service templates to quickly configure and rapid roll out new app services. It also supports replicate existing service templates and modification.	
	The proposed solution must have Single Pan dashboard to see WAF Policy, L7 DDoS Policy, BOT Protection attached to load balancing IP based on per application.	
	The proposed solution should have Domain/URL based Policy Configuration to override the security policy enforcement Mode for Learning and Blocking Settings for a defined unique identifier of Server Hostname + URL from Single Window Configuration panel.	
	The proposed solution must have an integrated	

RESTRICTED

	dashboard containing various features of alert and report generation including CPU, Memory , Connections , Throughput , Pool, Node,	
	The proposed solution must provide automated, real-time event alert mechanism.	
Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (three) year warranty for technical solution support with Patch & New Software Upgrade should be provided for the proposed solution.	
VM Resources	All the VM resources will provided by the customer, Bidder will provide the required software and license for central management solution.	

c. Backup Software (Subscription: 3 years)

Feature List	Feature Description	Bidder's Response
Brand	To be mention by the bidder (Preferably Commvault)	
Model	To be mention by the bidder	
Country of origin	As per tender specification Article no 20	
Country of Manufacture	As per tender specification Article no 20	
Supported OS platforms	Proposed solution should be available on various OS platforms and be capable of supporting backup/restores from various platforms including Windows, Linux and Solaris. Both Backup Management Server, Media Server and Client software should be capable of running on all these platforms.	
	Proposed backup solution must support ESX backup in non-windows environment, even without the need of windows backup server. There should not be any limitation from media server on supporting number of ESX/virtual guest host per media server.	
Renown brand	The Proposed Backup Software Must be present as Leaders in Gartner's Magic Quadrant for backup software.	
Features	Must support both source and target-based deduplication to meet specific workload demands.	
	Proposed Backup Software should be capable of supporting SAN based backup using client footprint instead of additional media/storage server footprint.	
	Backup Solution should support various level of backups including full, incremental, differential, synthetic, selective, block-level, optimized synthetic and user driven backup along with various retention period.	
	Proposed solution must provide Bare Metal Recovery, deduplication, encryption, database online backup, deduplication, backup data replication etc. with installation of single agent on clients. Multiple Agents/Binaries should	

RESTRICTED

	not be installed on the production Servers to achieve all above features.	
	Proposed Backup Software must provide both Fixed Length and Variable Length Data Deduplication to allow users choose the dedup option based on the backup workload.	
	Backup solution to support Cloud/object storage as Backup Target over generic S3 protocol.	
	Backup Software must provide Source (Client & Media Server) & Target base data Deduplication capabilities. It should provide Global deduplication across backup jobs and different workloads.	
Licenses	The proposed licenses should be minimum capacity of 100TB.	
	Necessary operating systems license for back systems should be provided	
Agent	The proposed backup solution must include Agent/ Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, MySQL, Exchange, Share Point and distributed databases/filesystems like NoSQL, MongoDB, Bigdata and Hadoop.	
Tape/disk-out backup	Backup Solutions should have capabilities to tape/disk-out backup catalog and deduplication catalog separately. Also, should be able to replicate all catalog information along with replication of backup images to DR site.	
Supported disk of Duplication feature	Deduplication feature should work with SSD, SAS, SATA and nearline SATA low cost disk technologies.	
high availability	Backup Solution management server which host the catalog should support high availability	
integration with virtual environment	The backup solution should support full integration to virtual environment like VMWare and Microsoft Hyper-V for the backup and recovery of full virtual machines and the individual files and folders inside them.	
Role-based access	Backup solution should support role-based access for administration	
Encryption	The backup solution should have support for 256 Bit AES Encryption.	
Data replication	The solution must support multiple site data replication without any additional license	
Backup scheduling	The proposed solution should be capable of doing backup scheduling with different RPO (Recovery point Objective).	
Link Aggregation	Proposed device should support link aggregation feature.	
Installation & Commissioning	Bidder should submit High-level, Low-level design documents directly from vendor.	
	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the network functional and shall provide respective documentation to IT Division.	

RESTRICTED

	Bidder should perform UAT and submit UAT signoff documents.	
	Bidder should submit project closure and operations documents to perform daily operations.	
Warranty/Support	The proposed solution should have 3 years OEM support with all software updates and patches.	
Training	Bidder should provide all necessary training for 6 person of BN for day to day operation & troubleshooting of the above solution.	

TECHNICAL SPECIFICATION OF PASSIVE HARDWARE**Passive Hardware for CDC**

1. Server Rack with KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1500 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	Ø 04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 1U Universal Horizontal Cable Manager	
	Ø 04 units 2U Universal Horizontal Cable Manager	
Vertical Cable Manager	At least 4 Vertical cable managers should be provided with each rack.	
Fixed trays/shelves	2 Fixed trays/shelves capable of caring at least 50 kg load, depth of at least 900 mm should be provided with each rack	
Sliding	1 Sliding trays/shelves should be provided with each rack	

RESTRICTED

trays/shelves		
Tool less Airflow Management Blanking Panels	At least 20 U blank panel should be provided with each rack	
Stabilization	Should be provided	
Rack Monitor	17" TFT rack mount APC/Vertiv/Arctiv or equivalent monitor which occupies only 1 U / 2U rack space 1 unit for each rack	
Integrated Keyboard and Mouse	Required with sliding functionality	
Power Distribution Unit (PDU) with built-in K-type transformer	Switched Rack PDU, 32A – At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
	Metered Rack PDU, 32A – At least 42 way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
KVM Switch	Switch that allows 2 users (one remote & one local User) single-point access and control of up to 16 multiple servers from a single console with 16 units KVM console cable and 16 units 1.5mtr cat 6 & 16 units 3mtr cat 6 patch cord	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each Rack to connect the servers/network/PDU equipment with the quoted rack.	
	02 units of C20 to industrial female (32A)	
	02 units of C19 to industrial male (32A)	
	02 units of C14 to industrial female (16A)	
	02 units of C13 to industrial male (16A)	
	04 units of C19 to C20 cable (16A, 3m).	
	10 units of C13 to C14 cable (10A, 3m).	
10 units of C13 to C14 cable (10A, 2m).		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

2. Rack without KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1200 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 1U Universal Horizontal Cable Manager	
	04 units 2U Universal Horizontal Cable Manager	
Tool less Airflow Management Blanking Panels	At least 20 U blank panel should be provided with each rack	
Stabilization	Should be provided	

RESTRICTED

Power Distribution Unit (PDU) with built-in K-type transformer	Metered Rack PDU, 32A – At least 42 way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
	Switched Rack PDU, 32A – At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.-	
	02 units of C20 to industrial Male (32A)	
	02 units of C19 to industrial Female (32A)	
	12 units of C19 to C20 cable (16A, 3m).	
	10 units of C19 to C20 cable (16A, 2m)	
	10 units of C13 to C14 cable (10A, 3m).	
	10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

3. Hot-aisle Containment System		
Feature List	Feature Description	Bidder Response
Brand name	To be mentioned (Preferably Schneider / Vertiv / Arctiv / Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Ducting Arrangements	There will be 02 types of Precision cooling available at CDC i.e Chiller based and DX based. A common ducting system should be used.	

RESTRICTED

<p>Containment Specifications</p>	<ul style="list-style-type: none"> a. The Aisle should be sized for two equal length rows of IT enclosures with supporting infrastructure with Top Cable Troughs. b. Hot aisle ducted configuration. c. Ceiling and duct panels must be constructed in a rectangular fashion and extend vertically. d. The Containment uses a series of polycarbonate panels, door frames and doors, and air blocks to enclose a Hot aisle zone which contains cooling unit supply air. e. All system components should be certified as suitable for this data center environment by documentation supporting UL Listings: UL484, CSA C22.2 No.236 and UL723S. 	
<p>Duct/AIR RETURN SYSTEM (as per design requirement)</p>	<ul style="list-style-type: none"> a. Should be 6.0 mm thick Lexan clear-ribbed panels or 2.36 mm thick V0 clear panels with aluminum framing/equivalent. b. Flame spread rates: Smoke development index "0-65" and flame spread index "0" in accordance with UL723 or ASTM84. Nominal thickness: 2.36 mm (V0 clear) – or-- Smoke development index "20" and flame spread index "0" in accordance with UL723 or ASTM84. Nominal thickness: 6.0 mm (Lexan) c. Minimum Light Transmission per ASTM D1003 equal to 82% or greater. d. Duct panels should be designed to be supported by the frames of the IT Equipment racks. Ceiling Panel frames sizes should be suitable to match up with various rack widths, row width, and hot aisle widths. e. The air return system should be designed to permit removal of the air blocks from within the contained zone without the use of tools for service access to the space above the Aisle. 	
<p>RACK EQUIPMENT BAYING KITS (as per design requirement)</p>	<p>Metal and plastic components should be supplied to establish consistent spacing between the racks or rack-based equipment, and to fill the space to provide an air containment seal at the juncture between two adjacent racks or rack-based equipment.</p>	
<p>DOOR FRAMES AND DOORS (as per design requirement)</p>	<ul style="list-style-type: none"> a. Door frames and doors shall be provided to establish air containment at the end of two rows of racks. The door frame system shall match the height of the rack based equipment, and match the design width of the contained aisle. b. Materials: Aluminum, SPCC and Tempered Glass. c. Doors shall be Sliding, to permit access into the contained aisle for maintenance or servicing. 	

RESTRICTED

	<ul style="list-style-type: none"> d. Doors shall be provided with a window, handles or latches. e. Two proximity switches provided per door for open/closed status f. Electronic Access Control: Smart PIN based,RFID g. LED Lights: Automatic lighting to sync to the automatic doors h. Automatic door closure system for sliding door i. Sliding Doors should be provided with swing-open functionality in case of emergency inside the aisle. 	
<p>FRAMES AND COMPONENTS SEALS (as per design requirement)</p>	<ul style="list-style-type: none"> a. Foam Rubber gaskets or metal/composite, brush, or plastic air blocks should be installed at Aisle joints to minimize open gaps between containment system components, such as door frames, ceiling and duct panels, and IT Equipment racks and rack-based equipment. Gasket and/or air blocks may include, but not be limited to, the following. b. Joints between adjacent ceiling/duct panels c. Joints between ceiling/duct panels and top of racks, if not metal to metal. d. Joints between door frames and ceiling/duct panels, if not metal to metal. e. Joints between door frames and racks at the end of the row(s). f. Joints between rack bottom rear frame and floor. g. Joints between duct panel and ceiling/roof of room. 	
<p>Air Return System (as per design requirement)</p>	<ul style="list-style-type: none"> a. Should consist of duct mounting rails and duct panels b. Mount to top of racks and extend up to ceiling plenum c. Allows for flexibility with overhead cabling and cable troughs d. Adjustable height supports e. Should support duct structure and extend duct upward to ceiling plenum f. Should mount to top of racks and rack height adapters g. Should be adjusted to be level with ceiling h. Should be placed every 600mm apart spanning length of aisle i. Should be provided with mounting bracket for various racks j. Should be provided with removable lexan or V0 airblocks and all necessary hardware to seal gap between top of racks and bottom duct rail k. Should be provided with Modular PDU and/or Rack Mounting brackets if needed 	
<p>Blanking Panels, Height Adapters, and Depth Extenders (as per design requirement)</p>	<ul style="list-style-type: none"> a. Blanking Panels should be placed where gaps between racks exist to seal contained aisle. The panel should match the height of the enclosures and match the width of the gap. It should not be mounted to any adjacent blanking panels nor should it b. support any adjustable height supports. 	

RESTRICTED

requirement)	<ul style="list-style-type: none">c. Depth Extenders should mount to front or back of enclosures to align aisle. The extender should match the depth of the adjacent racks and match the width and height of the enclosure (including any height adapters) of which it is being mountedd. Height Adapters should mount to the top of enclosures to align the enclosure height. The height adapter match the height of the adjacent racks and should match the width and depth of the rack (including any depth adapters) of which it is being mounted.e. Containment should Prevents short circuiting of cold air with warm airf. Provides even temperature across the cabinet height.g. Containment should Enhances equipment performance by increasing the temperature gradienth. Top Panel should comply to following points:i. Frame work should be CRCA Steel made of (600 mm / 800 mm wide)j. CRCA Steel is as per "IS 513 Grade D"k. Toughened Glass or Polycarbonate panel (Lexan panel)l. Doors (Sliding or Swivel) should comply to following pointsm. CRCA frame (1.2mm thickness) work and toughened glass (4mm thickness) or Lexan sheet (4mm thick).n. Sliding mechanism or Swivel mechanism with hinges.o. PU Foam Gasket should run across the edges of the door to prevent any leakage of cold air.p. Polyamide Cable Brushes are fitted at the bottom of doors to avoid leakage of cold air when doors are closed.q. All metal components should be power coated with Powder coat is with Nano ceramic pre-treatment process using a zirconium coat.r. The Powder coating process should be ROHS compliant.s. Powder coating thickness shall be 80 to 100 microns.t. Cabinet Rows should be either side of the Hot Aisle to be identical.u. Side Sealing Kits for cabinet to avoid air short cycling.v. Blanking Panels should be for unused "U" spaces.w. Side Panel should be plain i.e. without venting / perforation.x. Top Panels should be plain without Fans.y. Cabinet Front and rear door should be perforated.z. All the racks should be of same height.	
--------------	--	--

--	--	--

4. Automatic Voltage Regulator-800KVA		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Ortea/IREAM/ Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Capacity	800 KVA	
Input		
System	Three Phase	
Input voltage variation	±15 %	
Input voltage range	340-460 V	
Frequency	50Hz ±5% or 60Hz ±5%	
Max input current	1359 A	
Output voltage	400 V	
Rated output current	1155 A	
Efficiency	>98 %	
Adjustment speed	24 ms/V	
Control	Servo motor	
Standard features		
Voltage stabilization	Independent phase control	
Admitted load imbalance	100 %	
Ambient	-25/+45°C	

RESTRICTED

temperature		
Storage temperature	-25/+60°C	
Max relative humidity	<95% (non-condensing)	
Admitted overload	200% 2min.	
Harmonic distortion	None introduced	
Protection degree	IP 21	
Overvoltage protection	Class II output surge arrestors, Optimal voltage return through supercapacitors in case of black-out	
Communication ports:	RS232,RS485,Bluetooth, Ethernet, Slot for SNMP or equivalent.	
Remote Monitoring & Management:	SNMP based Remote monitoring capability and compatible with Data Center Infrastructure Management System (DCIM)	
Dimensions WxDxH	To be mentioned by the bidder	
Weight	To be mentioned by the bidder	
Installation & Commissioning	Installation, testing and commissioning with necessary accessories.	
MAF	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
Warranty	3 (Three) years full warranty (onsite covering everything with parts and services);	

5.Backup Online UPS Stand Alone-250KVA/KW; 30 Min Backup		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Country of Manufacture	To be mentioned	
Country of Shipment	To be mentioned	
Capacity	250 KVA/KW	
Input		
2+A44:A82	3Ph+N+PE	
Rated Voltage	380 / 400 / 415Vac	
Voltage Range For	<100% (-25%, +20%), <80% (-32.5%,	

RESTRICTED

loads	+20%), <60% (-35%, +20%)	
Input Frequency	40-70 Hz	
Total Harmonic	Distortion THDi < 3% for linear load THDi < 5% for non-linear load	
Input Power Factor	0.99	
Input Wiring	3Ph+N+PE	
Rated Voltage	380 / 400 / 415Vac	
Change over tolerance	± 30... ± 10% (Voltage) (According to VFI-SS-111)	
Input Frequency	50/60 ± 2/4% (selectable)	
Output		
Nominal Power	250KVA/KW	
Output Wiring	3Ph+N+PE	
Voltage	380 / 400 / 415 Vac ± 1%	
Frequency	Tracking the bypass input (Online Mode); 50/60 Hz ± 0.1% (Battery Mode)	
Waveform	Sine wave (THDv < 2% for linear load; THDv < 3% for non-linear load)	
Output Power Factor	1 (One)/Unity	
Efficiency	96,6%	
Overload Capacity	Inverter < 120% continuous; ≥ 125% for 10 min; ≥ 150% for 1 min Bypass 135% for long term; <1000% for 100ms	
BYPASS Efficiency	99.40%	
Operating Temperature	0-40°C (No power D rating)	
Storage Temperature	-40-70°C	
Relative Humidity	0%-95% (No condensing)	
Audible Noise	< 71 dB (Maximum)	
Communication		
LCD Display:	UPS shall have Minimum 6 inch (Diagonal) LCD Display for showing all necessary information Centrally. And individual LCD display for each module.	
Communication ports:	RS232,RS485,Bluetooth, Ethernet, Slot for SNMP	
Remote Monitoring & Management:	SNMP based Remote monitoring capability and compatible with Data Center Infrastructure Management System (DCIM)	
Battery Capacity	To be mentioned in Ah	
Brand	Any international Reputed Brand	
Model	To be mentioned	
Weight of Battery (Kg)	To be mentioned	
Backup Design	30 Min	

RESTRICTED

<p>Battery Cabinet</p>	<ul style="list-style-type: none"> a. The Cabinet architecture should be loading distributed and Compact height type. b. The Cabinet structure should be made with heavy load carrying material. c. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. d. The cabinet color should be best quality powder coated. e. A Circuit breaker metal box should be installed in the cabinet for isolating the battery. f. The breaker box should have an easy-to-open option. g. The Circuit Breaker Capacity should be as per OEM recommendation h. . Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
<p>Warranty</p>	<p>3 Years from the Date of Commissioning including the batteries</p>	

RESTRICTED

6.Modular Online UPS-200KVA/KW ; 30 Min Backup		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Country of Shipment	To be mentioned	
General Requirement	The vendor shall provide 2x200 KVA modular Hot Swap-able UPS in (N+N) configuration. The power cabinet must be of 250 KVA each. Also, each power cabinet shall be consisting of multiple numbers of hot-swappable power modules.	
Capacity	Minimum 200 KVA to be upgradable up to Min 250 KVA in a single cabinet.	
Module	Each Module will be minimum 25KW Hot Plug and hot swappable function	
Number of Module	To be mentioned	
Backup Time	Minimum 30 min at 200 KW full load from factory fitted hot-swap-able battery pack.	
Input Battery Voltage	Select-able and Configurable	
Topology	Modular, True Online Double Conversion with Distributed/ Decentralized Active Redundant Architecture	
Input Power factor	Minimum 0.99 at full load	
Output Power factor	1 or unity	
Input		
Input Wiring	3Ph+N+PE	
Rated Voltage	380/400/415Vac	
Voltage Range	For loads <100% (-25%, +20%) <80% (-32.5%, +20%) <60% (-35%, +20%)	
Input Frequency	40-70 Hz	
Total Harmonic Distortion	THDi<3% for linear load, THDi<5% for nonlinear load	
Bypass		
Input Wiring	3Ph+N+PE	
Rated Voltage	380/400/415Vac	
Input Frequency	50/60 ±2/4% (selectable)	
Input Feed	Duel	

RESTRICTED

Output		
Output Wiring	3Ph+N+PE	
Rated Voltage	380/400/415Vac	
Frequency	50 Hz / 60 Hz	
Waveform	Sine wave (THDv<1% for linear load THDv<3% for non-linear load)	
Overload Capacity	Inverter 124% continuous 125% overload for 10 min 150% overload for 1 min, Bypass 135% overload for long term <1000% overload for 100ms	
Crest factor	3:01	
General Features		
Features of individual Modules of Modular UPS system:	Individual rectifier, inverter, Control Logic, Static Bypass, On/Off Switch and LCD Display.	
Redundancy, Fault tolerance and Fault Isolation	The UPS System shall Design for no single point of failure and should be driven by the different modules. It will not consist of any major component failure of which may cause the failure of all module's operations. It shall have fault isolation capability. True hot Swap-able function.	
Controller	Separate controller for each module.	
Alarm/Status Indicator	Alarm/Status Indicator for each module.	
Mechanical Bypass	Central mechanical bypass switch	
Battery Connection	Please mention	
Supported Battery Type	Lithium-Ion and VRLA	
Efficiency (VFI)	Minimum 97 %	
Environment		
Protection rating	IP 20 or Better	
Operating Temperature	0-40°C or To be mentioned	
Relative Humidity	To be mentioned	
Audible Noise	< 65dB or Better	
Communication		
LCD Display:	UPS shall have Minimum 6 inch (Diagonal) LCD Display for showing all necessary information Centrally. And individual LCD display for each module.	
Communication ports:	RS232,RS485,Bluetooth, Ethernet, Slot for SNMP	
Remote Monitoring &	SNMP based Remote monitoring capability and compatible with Data Center Infrastructure	

RESTRICTED

Management:	Management System (DCIM)	
Standard:		
Safety:	IEC/EN 62040-1	
Electromagnetic Compatibility	IEC/EN 62040-2	
Performance	IEC/EN 62040-3	
Manufacturer Certification	ISO 9001/ ISO 50001	
UPS Cabinet Weight & Dimension		
Weight	To be mentioned	
Dimension - WxHxD (mm)	To be mentioned	
Battery Specification		
Battery Type	Lithium-ion	
Brand	Please mention	
Model	To be mentioned	
Country of Origin	To be mentioned	
Country of Manufacture	To be mentioned	
Nominal Voltage	To be mentioned	
Battery Module	The UPS shall have hot swap-able battery module. Can be run with Lower/Higher number of Battery module.	
Battery Amp	To be mentioned	
Number of Batteries	To be mentioned	
Weight per Battery (Kg)	To be mentioned	
Battery Dimension	To be mentioned	
Designed Life Time for Battery	Minimum 15 Years	
Battery Cabinet	External type best quality battery cabinet with circuit breaker, Controller with required electrical/electronic components, Battery Monitoring System and shielded battery module.	
Battery Cabinet Dimension	To be mentioned	
Battery Monitoring System (BMS)	UPS Shall have Battery Monitoring System that capable to monitor individual battery voltage, Battery Impedance (Ohmic Value), temperature, health etc. with graphical report.	
Installation	Supply, installation, testing, and commissioning by	

RESTRICTED

	OEM-certified engineer.	
Warranty	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

7. 40KW Online UPS for Security Items with 30 Minutes backup		
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity:	Minimum 40 KW	
Output power factor:	1 (One)	
Topology:	True online double conversion	
Parallel Configuration:	Up to 4 units	
Input		
Voltage range:	110~280 Vac (Single + G)	
Frequency range:	45-70Hz (auto sensing)	
Input power factor:	≥ 0.99 @ 100% linear load	
Input Current Distortion:	≤ 3% (full load)	
Output		
Output voltage:	200/208/220/230/240 Vac (Single + G)	
Output voltage distortion:	<1%@100% Linear Load; <3% @100% Non-Linear Load	
Output voltage regulation:	±1%	
Frequency range:	±1Hz or ±3Hz (selectable)	
Output waveform:	Pure sine wave	
Overload Capacity Inverter:	<105%continuous 105-125% for 600 to 30 seconds	
	transfer to bypass. 125-150% for 30 seconds to immediately transfer to bypass.	
EFFICIENCY:	94%	
High Efficiency Mode:	≥98%	
ENVIRONMENTAL:	Operation Temperature 0~40°C / 32~104°F	

RESTRICTED

Operation Humidity:	20~95%RH (without condensing)	
Altitude:	1000m/3280ft without derating"	
STANDARDS AND CERTIFICATION S:	Safety: IEC / EN62040-1, UL1778; EMC: EN62040-2, EN61000-3-2, EN61000-3-3	
FCC Class A Performance:	IEC / EN62040-3	
Manufacturing:	ISO 9001:2015, ISO 14001:2015 / CE, UL, cUL, FCC	
Battery Capacity:	To be mentioned in Ah	
Brand:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20a	
Country of Manufacture:	To be mentioned	
Model:	To be mentioned	
Weight of Battery (Kg):	Please mention	
Battery Cabinet:	<ul style="list-style-type: none"> a. The Cabinet architecture should be load distributed and Compact height type. b. The Cabinet structure should be made with heavy load carrying material. c. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. d. The cabinet color should be best quality powder coated. e. A Circuit breaker metal box should be install in the cabinet for isolating the battery. f. The breaker box should have an easy-to-open option. g. The Circuit Breaker Capacity should be as per OEM recommendation. h. Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

RESTRICTED

8.Isolation Transformer 250KVA		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Ortea/IREAM/ Equivalent)	
Model	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Rated power:	250kVA	
Input Voltage	3PH+N 400 Vac	
Output voltage:	3PH+N 400 Vac	
Type	Dyn11 – K20	
Windings	Copper	
Bypass	Inbuilt Maintenance By pass	
Fittings	Input and Output Circuit Breaker & Pilot Lamp	
Warranty	3 Years from the Date of Commissioning	

9. Floor Mounted Power Distribution System-200A with Auto transfer Switch for Server room		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Maximum Total Current Draw per Phase	200A	
Nominal Input Voltage	400V 3PH	
Input Frequency	47 - 63 Hz	
Rack Height	To be mentioned	
Features	Multiple distribution options (3-phase and 1-phase)	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Local and web-based monitoring: Status available to customers both in the data center and remotely	
	Current Monitoring: Monitors the aggregate current draw per power distribution unit.	
	Network management capability: Full-featured network management interfaces that provide standards-based management via Web, SNMP, and Telnet.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
	Modular design: Provides fast serviceability and reduced maintenance requirements via self-diagnosing, field-replaceable modules.	
Auto Transfer Switch (3-Phase) Features	Minimum 2 incoming capable of 200A current per phase from bus-bar.	
	1 outgoing capable of 200A current per phase to Floor Mounted Power Distribution System.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	

RESTRICTED

Certificates	Machine must comply tier-3 (Uptime Institute/epi) compliance in all aspects	
Warranty	Three (03) years full	

10. Floor Mounted Power Distribution System-100A with Auto transfer Switch for MMR-01&02		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Maximum Total Current Draw per Phase	100A	
Nominal Input Voltage	400V 3PH	
Input Frequency	47 - 63 Hz	
Rack Height	To be mentioned	
Features	Multiple distribution options (3-phase and 1-phase)	
	Tool-less installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Local and web-based monitoring: Status available to customers both in the data center and remotely	
	Current Monitoring: Monitors the aggregate current draw per power distribution unit.	
	Network management capability: Full-featured network management interfaces that provide standards-based management via Web, SNMP, and Telnet.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
	Modular design: Provides fast serviceability and reduced maintenance requirements via self-diagnosing, field-replaceable modules.	
Auto Transfer Switch (3-Phase) Features	Minimum 2 incoming capable of 100A current per phase from bus-bar.	
	1 outgoing capable of 100A current per phase to Floor Mounted Power Distribution System.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network	

RESTRICTED

	Management System.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 (Uptime Institute/epi) compliance in all aspects	
Warranty	Three (03) years full	

11. IT Power Distribution Module 3x1 Pole 3 Wire 32A (1-Phase 32A Industrial Socket)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	230V	
Output Connections	(3) IEC 309 32A (2P+E)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-	

RESTRICTED

	assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

12. IT Power Distribution Module 3 Pole 5 Wire 32A		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 32A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-	

RESTRICTED

	assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

13. IT Power Distribution Module 3 Pole 5 Wire 63A		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	63A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 63A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power	

RESTRICTED

	Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

14. Rack Automatic Transfer Switch for single corded equipment		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Type	Automatic switching power redundancy to single corded equipment	
Form factor	Rack mountable horizontal 1U or 2U solutions	
Manageability	Network manageable through TCP/IP	
Transfer Time	Zero	
Capacity	At least 6 kW or higher	
LCD display for operating information	Should be inbuilt with the system.	
Ports	At least 6 ports or Higher	
Software and Interface	ATS Monitoring and Management Software and Ethernet interface from each ATS.	
	Provided software's functions should include monitoring and Controlling the ATS remotely through TCP/IP	
Firmware upgrades	On-the-fly firmware upgrades should be possible	
Event logging	Event logging with graphs should be possible in the proposed software	
Cables	12 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.	

RESTRICTED

	04 units of C20 to industrial female (32A)	
	02 units of C14 to industrial female (16A)	
	04 units of C19 to C20 cable (16A, 3m).	
	02 units of C19 to C20 cable (16A, 2m)	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

15. Transient Voltage Surge Suppression (TVSS)		
Feature List	Feature Description	Bidder Response
Brand	To be Mentioned (Preferably Schneider/ Rayvoss / Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Operating voltage, current and frequency	To be mentioned	
Features	Microprocessor-based controller	
	Plug-in modules for easy replacement	
Visual Indication	To be mentioned	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3/rated-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

16. Signal reference grid system	
Feature Description	Bidder Response
A separate & complete SRGS is to be installed in accordance with applicable codes & standards for data center, MMR-01&02, Power room-01&02.	
2. Separate SRG sub system for both MMR is to be design & combinedly will be connected with separate earthing system(N+N, 1 ohm each).	
Separate SRG system is to be design for server room (All Server racks) with separate earthing system (<1 Ohm).	
Separate SRG sub system for both Power room is to be design & combinedly will be connected with separate earthing system (<1 Ohm).	
Grid pattern of SRG will be followed the mesh system to secure floor pedestal	
In SRG system proper copper strip, grounding clamp, UL listed bonding grids, low impedance raiser kit, BCF weld, BHO weld, Flat strip pedestal ground clamp, CPC pipe clamp are to be used.	

17. Data Center Earthing & Bonding system		
Feature List	Feature Description	Bidder Response
Bonding	Proper bonding for data equipment rack, telecommunication backbone, power cabinets, is to be designed & installed.	
	Proper & separate bonding network for power equipment, server rack, cooling system has to be interconnected with separate earth termination/ grounding system.	
	Bonding connection at all SRG mesh intersections & bonding between mesh & equipment is to be confirmed.	
SRG and Grounding	SRGs: The signal reference grid (SRG) system to be implemented for server room, MMR room and power room separately.	
	Ground Resistance: The ground resistance has to be below 1 ohm.	
	General Requirement: All metallic object including cabinet, PDUs, Cooling system, raised floor etc. should be connected to grounding system.	
	For Rack/cabinet continuity	
	Racks should be assembled with paint piercing grounding washers, under the head of the bolt and between the nut and rack, to provide electrical continuity.	
	A full-length rack-grounding strip should be attached to the rear of the side rail with thread-forming screws to ensure metal to metal contact.	

RESTRICTED

	For Rack/Cabinet Grounding: Larger bonding conductor to bond each rack or cabinet with the grounding strip to the data center grounding infrastructure(SRG System)	
	For Telecommunications Grounding Bar	
	Provision of larger conductor to bond the data center grounding infrastructure to the TGB.	
	Two hole copper compression lugs are preferred for vibration.	
	Telecommunications Bonding Bar	
	The TBB should be installed as a continuous conductor, avoiding splices where possible.	
	Avoid routing grounding/earthing conductors in metal conduits.	
	Telecommunication Main Grounding Bus Bar	
	The TMGB is to be bonded to the service equipment (power) ground, which connects to earth ground (the grounding electrode system)	
	Supplier need to consider earthing meter installed to the separate earthing group for DC equipment(Present & Proposed data center)	
Warranty	10 years	

18. Data Centre Infrastructure Management system (DCIM)with energy & environment monitoring system with BMS		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Sunbird/Commscope/Equivalent)	
Model name	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
No of device license required	At-least 1500 node license (If more no. of license is required to cover the full Data Center as per given requirement, have to be included)	
	If the proposed system is an appliance based, the appliance should be provided.	
Room Monitor	12	
Room Sensor	12	
Rack Monitor	72	
Temperature and Humidity Sensor with digital display	50	
Temperature and Humidity Sensor	36	

RESTRICTED

Spot Fluid Sensor	30	
Smoke Sensor	50	
Alarm beacon	5	
Vibration Sensor	10	
Door Switch Sensor for Rack	36	
Door Switch Sensor for Room	12	
Tablet with pre-loaded Application	03 (at least 7 inch)	
	All material and equipment used shall be standard components, regularly manufactured, available and not custom designed especially for this project. The data center infrastructure system, including the DCIM, shall previously be thoroughly tested as a system, and proven in actual use prior to installation on this project	
	The DCIM shall be installed on a physical server, or as a virtual appliance, with a specified HTTP or HTTPS connection to access the user interface (DCIM client), and standard TCP protocol connections for communications with the monitoring system	
	The DCIM system-level redundancy and load-balancing shall be provided using a server-level cluster setup. Up to 4 servers should be setup in a cluster to gain performance improvements	
	The DCIM shall enable vendor-neutral inventory management with real-time device failures and data shown within a data center physical layout. Graphical floor layout and rack elevation view shall be supported from Day 1	
	The DCIM tool shall provide location-based drill-down views providing a structured overview of data center locations, from a global to local view down to single assets.	
	A Power Usage Effectiveness (PUE) dashboard will provide information on daily energy use	
	Inventory report provides structured information on all rack-mount devices, organized by device type, age, manufacturer, and properties for quick overview of all current devices within a particular data center	
	The DCIM tool shall have a search capability to allow data center operations to quickly locate a piece of equipment in the rack layout and floor layout.	
	The DCIM tool shall provide public web services API to allow third-party applications to access the inventory database, alarms and events, capacity and cooling analysis data, and PUE information	
	The DCIM shall provide provisions to predict the	

RESTRICTED

	optimal location for physical infrastructure and rack-based IT equipment based on the availability and requirements of physical infrastructure capacity and user defined requirements such as redundancy, network, and business use grouping	
	The DCIM shall provide provisions to reduce stranded capacity and enable informed decision making and planning by proactively analyzing the impact of future moves, adds, changes before they occur, ensuring that the physical infrastructure provides the required space, power, and cooling capacity for current and future needs	
	The DCIM shall be capable of hosting additional add-on modules that allow a user to perform energy efficiency and energy cost management, inventory management, power and cooling capacity management, change management, IT optimization, IT power capping, server access (software Keyboard Video Mouse or KVM), dynamic cooling control and mobile data center management	
	The DCIM shall provide read-only smart phone applications to get a high level status of the data center operations and KPI	
	The DCIM shall be capable of integrating with additional plug-ins that supports Cisco UCS Manager, HP OneView, Vigilent dynamic cooling control, BMC Remedy ticketing system, Microsoft System Center Virtual Machine Manager 2008/2012, HP uCMDB, and VmwarevCenter, etc.	
DCIM Operation	The DCIM software shall provide the methodology to create visual view of the data center floor layout, and the racks view and the equipment within, and manage network connectivity. This module shall also map the alarms to the appropriate device on the floor layout. The DCIM software shall support the following capabilities -	
	Floor Layout	
	The DCIM tool will have the capability to add locations and rooms of different types to the data center model to represent the actual physical enterprise infrastructure.	
	The DCIM tool will have the capability to configure a bird's eye view of the room layout to ensure the layout in the data center model accurately represents the real-world physical environment of the room. This includes any physical attributes of the room such as size, shape, doors, windows and walkways.	
	The DCIM tool will have the capability to see multiple rooms in a layout pane at the same time allowing a user to compare or drag equipment between them –	

RESTRICTED

	for modeling.	
	The DCIM tool will have the capability to export the complete or filtered data center inventory into a delimited file (.csv file).	
	The DCIM tool will have the capability to render the floor layout in both 2D and 3D view.	
	Ability to import an AutoCad (.dwg) floor drawing and display the floor layout. Each layer can be toggled on or off. Rooms can be created based on wall detection on the AutoCad drawing.	
	Ability to export the Floor Layout to AutoCAD format (.dwg). Each overlay and the information in the overlay must be stored in individual layers.	
	Ability to export the Floor Layout to the following picture formats: BMP, JPG, PNG and SVG.	
	Ability to export the Rack View to the following picture formats: BMP, JPG, PNG and SVG.	
	Ability to copy/paste equipment on the floor, such as racks, PDUs, UPS and cooling units as well as equipment in the racks, such as servers and patch panels. You can	
	copy/paste individual pieces of equipment or multiple items, such as a rack and its contents.	
Multi-tenant Data Center Support	Ability to create cages and auto-detect cage area in square meters or square footage.	
	AutoCAD drawing through cage selection and wall detection.	
	Ability to assign customer to data center asset including rack mounted equipment, racks, cages, etc.	
	Cages, racks and servers are color coded based on sales status (closed, reserved, internal, and open).	
	Ability to assign Contracted Power value to each cage, rack or server.	
	Ability to add power receptacles to each cage.	
	Show a legend on the floor view with information about how many racks are open, closed, reserved and internal.	
	Show a legend on the floor view with information about how much space is open, closed, reserved and internal.	
	Show a legend on the floor view with information about total room area, sellable space and space efficiency.	
	The DCIM tool will identify how much weight has been placed in a rack / room compared to the predefined load bearing capability settings of the rack.	

Rack elevation View	Illustrate the weight of the equipment added to the rack in the rack layout compared to the maximum equipment loading capability of the rack.	
	Visualize status of network ports on equipment (used vs. not used).	
	Visualize network cables.	
	Network Management	
	The DCIM tool will be able to model the configured network connections and allows a user to setup new network routes between the configured equipment.	
	Network port properties will have the capability to be imported from a product catalog and/or will be user configurable.	
	Ability to configure network routes for selected network equipment in the layout, for example between a server and a switch or a switch and a switch. A route is defined as a connection from a piece of equipment (communication endpoint, such as a server or layer 2/3 network gear, such as a switch) to the first piece of equipment that is a communication endpoint or layer 2/3 network gear.	
	Ability to configure cable types and color code each cable type.	
Product Catalog	The DCIM tool will be able to provide a product catalog that contains up-to-date floor and rack mounted data center equipment.	
	The DCIM tool will be able to allow a user to add floor and rack-mountable equipment to a rack, server room, electrical room or store room.	
	Ability to create an inventory bundle that combines multiple pieces of equipment in one building block.	
Dashboard Key Performance Indicator (KPI) View	Provide a map view to monitor the data center operations in a quick overview, including any alarms in different locations and rooms.	
	From the map overview, one can drill down to locations > rooms > racks > servers for details or troubleshooting.	
	Display capacity KPIs for each data center in the map view. The KPIs should include the status of the Power, Cooling, U-space and Network utilization.	
	Power is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	
	Cooling is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	

RESTRICTED

	U-space is represented as the percentage of the available U-positions (U-pos) that is populated with equipment in the location or room.	
	Network is represented as the percentage of the available Network ports (ports) that is utilized by networking equipment in the location or room	
<p>Data Center Operation: Capacity</p> <p>Capacity Planning</p>	The DCIM software shall provide capabilities to perform capacity planning, create capacity groups, perform power and cooling analysis as per the following details:	
	The DCIM software will provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, network and power capacity to optimize capacity utilization and avoid stranded capacity:	
	Impact simulation: Generates a list of equipment that would be impacted if the selected piece of equipment, e.g. a UPS or cooling unit, was to fail.	
	Measured Load: Display measured load data for UPS and racks in the floor layout that identify how much of each UPS or rack's maximum kW power is in use. This requires communication to power monitoring devices or servers.	
	Measured Load: Displayed measured load data for cages in the floor layout that identify how much of a cage's contracted power is in use. This requires communication to power monitoring devices or servers.	
	Power Capacity: Ability to assign planned capacity for each rack and illustrates rack capacity consumption compared to the planned recommended values for that rack. Provide information such as remaining power, the amount exceeding the recommended capacity.	
	Power Path: Ability to model power connections between the equipment supplying and delivering power and the equipment requiring power. This includes power path from switchgear, UPS, main PDU with modular circuit breaker mapping, rack RPDU and to individual servers.	
	Power Path: Ability to export the power path to a comma separated file.	
	Rack U Space: Ability to monitor and display rack U space utilization of each rack.	
	Ability to model capacity groups that allows a user to group equipment's, placing it in groups of racks with similar power capacity requirements to match the IT equipment with availability needs and avoid stranded space, power, and cooling capacity. For example, group a set of high-density racks together for	

RESTRICTED

	optimized power and cooling configuration.	
Power Analysis	Ability to detect the following list of configuration issues regarding data center power configuration and provide recommended actions:	
	Connection has not been configured between PDU and power supply: A power connection is missing in the data center model from this PDU to the power supply from which it should receive power.	
	Equipment connected to this PDU draws more power than is supported by the power supply breaker: The breaker does not provide sufficient power to cover the power requirements of the equipment connected to that PDU.	
	Equipment is connected to a rack PDU outside this rack: The power connection setup for this equipment is not optimum as it is setup to be supplied by a rack PDU that is not positioned in the same rack as the equipment.	
	Internal redundancy setup for UPS and group must match: The internal redundancy setup for the UPS and group does not match, for example N and N+1.	
	Rack is without rack PDU or a rack PDU is not powered: The rack is without rack PDUs or its rack PDUs are not connected to a PDU, remote distribution panel (RDP) or power panel.	
	The breaker configuration does not support rack's estimated load: The equipment in the rack draws more power than the breaker supports. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.	
	The input voltage setting required by the equipment is not available in current rack: In the data center model, the server's input voltage requirement cannot be supplied by the rack PDU in the rack.	
	The measured load exceeds the estimated load per phase designed for the rack: Connected devices in the rack use more power than the estimated load per phase in the rack shall be indicated in the data center model.	
	The measured load exceeds the total estimated load configured for the rack: Connected devices in the rack that use more power than the total estimated load in the rack shall be indicated in the data center model.	

RESTRICTED

	<p>The measured load of the UPS exceeds the total estimated load of the connected equipment: Devices connected to the UPS use more power than design capacity or they have not been assigned to the correct UPS in the data center model layout to correctly represent the physical infrastructure. In case of 3 phase equipment, the problem shall be indicated even if the measured value is only too high for one of the phases.</p>	
	<p>The phase configuration for the connected server is not supported by the rack PDU: The phase connection configured for this server is not valid. This message will occur if a power connection had been configured to this server but subsequently changes have been made to the phase configuration.</p>	
	<p>The Rack PDU output voltage setting does not match the output voltage of the connected PDU / Power Panel: The power connection is invalid because the voltage required by the rack PDU is not available from the power distribution component.</p>	
	<p>The server must be supplied from the same phase from both distribution units: The redundancy setup requires identical phase distribution setup for A and B feed.</p>	
	<p>The UPS in the layout does not supply enough power to match the configured load of connected equipment in the layout: The load of the equipment connected to the UPS is higher than the load that the UPS can supply. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.</p>	
<p>Cooling Analysis</p>	<p>The DCIM software shall be able to calculate cooling performance of data centers in real-time with CFD-like simulation, provide calculated inlet and exhaust temperatures per rack plus capture index (percentage of heat captured by cooling devices) per rack.</p>	
	<p>Ability to present the calculation results visually in the floor layout.</p>	
	<p>Ability to alarm cooling configuration issues and provide recommended actions. For example, a room has no perforated tiles for the Computer Room Air Conditioning (CRAC) unit airflow (one or more CRACs have been added to the floor but no perforated tiles have been added), or there is no perforated tile airflow (one or more perforated tiles have been added to the room but no CRACs have been provided to supply any airflow).</p>	
	<p>2D plenum airflow and pressure view: Provide a 2D under-floor plenum view that shows airflow vectors and Cubic Feet per Minute (CFM) based on the height</p>	

RESTRICTED

	of the raised floor, the placement and type of perforated tiles and cooling devices. When a cooling unit or a perforated tile is moved around, the flow vectors and airflow CFMs shall update instantly.	
	3D temperature and airflow view: Provide a 3D view showing max/average inlet/return temperature and airflow above the raised floor. Calculate velocity vector and temperature in real-time (seconds) to allow customers to try what-if scenarios. Ability to slide the temperature and velocity plane in all three dimensions.	
	Ability to simulate failure of one or more cooling units and examine impacts to IT equipment.	
	Ability to map temperature sensors to rack elevation or anywhere in the data center 3D space and draw the 3D measured temperature map based on the measured data.	
Integration with 3rd Party Software	The DCIM software shall support integration with Cisco UCS manager to retrieve real-time power measurement data for blade servers and display them. In addition, it should support automatic power capping Cisco UCS chassis based on rack PDU breaker setting to safe guard rack PDU breakers.	
	The DCIM software shall support integration with VMware Center and Microsoft System Center Operations Manager (SCOM), Virtual Machine manager to retrieve virtual machine information and map them to physical servers.	
	The DCIM software shall support integration with HP Universal Configuration Management Database (uCMDB), pushing IT asset data such as network, server devices and properties to the DCIM software.	
	Ability to support two-way data exchange between the DCIM software and a broad range of systems, such as CMDBs, asset management systems, and building management systems using Extract, transform and load (ETL). Based on the ETL system, it is possible to develop custom solutions, integrating DCIM with a broad range of data sources.	
Data Center Operation: Energy Efficiency	The DCIM shall provide the following functionality from the data center Energy Efficiency point of view	
	The DCIM tool will provide current and historical Power Usage Effectiveness (PUE) values and full insight into current and historical energy efficiency.	
	It will present how much power is devoted to driving the installed IT-equipment compared with the total facility consumption.	
	Identify efficiency losses and enables improved PUE at the subsystem level.	
	Provide insight into energy losses and cost of energy at the subsystem level, providing details of which subsystem	

RESTRICTED

	draws the most costs.	
	The DCIM tool will have a web-based dashboard view which includes efficiency data on current and historical PUE, as well as detailed subsystem cost analysis.	
	The DCIM tool will provide a report on current and historical PUE values.	
	The DCIM tool will provide energy efficiency analysis, PUE and DcIE (Data Center infrastructure Efficiency) reporting.	
Data Center Operation: Change	The DCIM shall provide the following change management functionality to keep track of additions, movements, maintenance or deletions in a data center:	

19. Controlled electric lighting system (Electric lighting & Emergency Lighting)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Features		
Data Center Lighting & cabling	The data center automatic & manual lighting system with required cabling is to be design & installed by bidder. Lighting & interior design must be vatted from BNNET acceptance committee.	
Emergency Lighting Control	When the normal AC power fails, the emergency lighting system should sense the power failure and immediately switches to the emergency mode, illuminating more than 5 lamps at a time.	
	When AC power is restored, the emergency lighting system should return to the charging mode until the next power failure	
No of Emergency Light	To be mentioned	
Central Control Panel	The central control panel should include all the power lighting and also the emergency lighting for allowing monitoring and control of Data center lighting system.	
Total Floor Area	As per drawing	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	

RESTRICTED

Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

20. Electrical Works		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Electrical DB Panels & DB Accessories		
	Supply & installation of Electrical Panels housed in 2.0mm standard sheet steel enclosure type tested, fixed Type, compartmentalized, totally enclosed, free standing, Floor mounted type, dust and vermin Proof, duly wired up and ready for installation at site. All MCB, MCCB & ACB should be lcs 100% lcu. The boards are designed and constructed in accordance with IEC61439-6. Busbars and other live parts are spaced and insulated in accordance with IEC standard. All DB should C911:C925	
	The DB system should have following features: a. Factory assembled power distribution module with breaker position monitoring. b. No rear access c. Network management via web interface, SNMP, modbus and other appropriate interfaces. d. Compatible with Tier -3 data center. e. Self diagnosing module and tool less module replacement f. Output metering and branch circuit/current monitoring. h. Local access display interface	
	Technical Description	
AVR Output DB-01	Bidder will design & proposed required DB for AVR, Online UPS, HVAC, FMPDU, others utility load as per attached to comply with tire-3 Standard. During design bidder will consider appropriate bus bar, breaker, protection devices, monitoring devices for SCADA/DCIM monitoring.	
AVR Output DB-02		
MDB-01		
MDB-02		
HVAC DB-01		
HVAC DB-02		
BACK UPS O/P DB-01		

RESTRICTED

BACK UPS O/P DB-02		
SECURITY DB-01		
SECURITY DB-02		
FLOOR DB-01		
FLOOR DB-02		
UPS O/P DB- 01		
UPS O/P DB- 02		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

21. Power Cabling and Others related works		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably BRB/ Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Cable Requirements	Bidder's has to quote cabling for complete Data Center.	
	All connection of UPS, AVR, RACK and other electric items (approx. 36 Nos. Rack) inside the data center through IT Power Distribution Modules.	
SLD Diagram	Bidder has to provide Complete SLD starting from Sub-station to IT load	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

22. Power Cable Ladder		
Feature List	Feature Description	Bidder Response
Brand	To be mention	
Model	To be mention	
Origin	As per Tender Specification Article no 20	
Country of Manufacturing	As per Tender Specification Article no 20	
Type	Metal Steel/Stainless Steel Mesh Type Electrical ladder	
Cable ladder size	width 12"	
Height	Approx. 2"/Customized	
Materials	U Steel cable ladder with electro zinc plated treatment. Thickness: Min.1.6 mm and average load of more than 200KG per meter.	
Color	Powder coating White or Silver or Siemens Gray	
Installation material	Thread Rod/Hanger (max 3'), Flat BAR, Clump, Royal Bolt, Screw, Saddle, bending/L-shape, T-Shape etc. for hanging/vertical /Horizontal area both the overhead and under raised floor	
Power Cable Tray	Cable Tray	

23. Electrical Switch Sockets		
Feature List	Feature Description	Bidder Response
Electrical Switch Sockets	Brand: To be mentioned	
	Country of Origin: To be mentioned	
Industrial Socket 32A SP	Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge	
	Supply and installation of imported gang switches& socket and wall boxes complete with all other necessary accessories and connections everything complete as per drawing, specification and instruction of the Engineer-in-charge. The wall boxes may be locally made of 18SWG galvanized steel sheet including earthing block. (Maximum Current 13 Amps)	
	3-Pin wit 2 pin socket	
Switch for Light	Supply and installation of imported 13A, 220V, combined switched socket outlet including the box,	

RESTRICTED

	cover plate with necessary galvanized machine screws, earthing block complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge. The box may be locally made of 18SWG galvanized sheet steel. Maximum Current 10 Amps	
	3 Gang Switch	
	4 Gang Switch	
	2 Gang Switch	
Lighting System	Supply of ceiling surface/concealed mounted light fixture complete with energy saving LED light, best quality lighting shade with mounting kit and all other necessary materials as per drawing, specifications and direction of the Engineer-in-charge.	
	Recessed Ceiling Luminaires, Series for LED panel light 2'x 2' with hanging accessories	
Emergency light with battery back up		
Brand:	Any international Reputed Brand	
Model:	To be mentioned by bidder	
General Features	Emergency light luminaire	
	Input: 220VAC +/- 10% 50 Hz 1 phase	
	Bulbs: 2 x 9W & 12 W SMD LED super wide beam 90 Deg.	
	Lamp: Aluminum heat sink body and plastic diffuser 180 Deg. Adjustable legs	
	Automatic solid-state system	
	Constant current charger	
	10-12 Hours charging duration	
	Battery Nickel Metal hydride (Ni-MH)	
	Battery protection: Low voltage cut off	
	System protection: high voltage cut off	
	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: front cover 1.5mm electro-galvanized steel sheet with epoxy powder coated and stove enamel	
	Operation temperature: 10 Deg. - 40 Deg.	
	IP rating: IP 20	
Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)		
TIS.1102-2538 (self-contained emergency light Luminaries)		
Emergency Exit Sign	Wall and ceiling mounted	
Brand	Any international Reputed Brand	
Model	To be mentioned by bidder	
General Features	Input: 220VAC +/- 10% 50 Hz 1 phase	

RESTRICTED

	Lamp: SMD Surface mount	
	Automatic solid state system charger	
	Constant current charger	
	10-12 Hours charging duration	
	System protection: high voltage cut off	
	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: Electro-galvanized steel sheet 1mm & front plate 1.5mm epoxy powder and stove enamel coated anti-rust corrosion proof	
	ISO green legend	
	Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)	
	TIS.1102-2538 (self-contained emergency light Luminaries)	
Electrical Accessories	Accessories: Lugs, Heat Shrink, Cable tie, Screw, GI wire, Royal Plug, Royal Bolt, Clump, PVC Tape, Masking Tape, Rivet, High Quality nylon Fastener etc.	

24. Precision Air Conditioner (PAC)_DX for Server Room		
Products Names/Items	Description of requirements	Bidder Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	USA/UK/EU	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 104 kW	
Total sensible capacity	Minimum 104 kW	
Net Total Capacity	Minimum 98.0 kW	
Net Sensible Capacity	Minimum 98.0 kW	
Air Flow (Indoor)	Minimum 26,500 m ³ /h	
Air Flow(outdoor)	Minimum 31,200 m ³ /h	
Ambient	45 °C	

RESTRICTED

Temperature		
Fan Technology	EC Fan Technology	
Electrical power consumption	Maximum 11.1 kW/Compressor.	
Energy Efficient Ratio (EER)	3.63 kw /better	
AER	0.25 W/(m ³ /h)	
Total power consumption	Maximum 28.8 kW	
LpA (2m free field)	Indoor: 65.4 dB(A)	
LpA (5m free field):	Outdoor: 57.9 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50%	
Altitude above sea level:	100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 3 (three)	
Heat rejection	63.6 kw (per compressor)	
Condenser capacity	63.6 kw each condenser	
Compressor type	Scroll Type	
Expansion Valve	Electronic	
Electrical Heating	9 to 18 kw or more	
Steam humidification	8 to 15 kg	
Refrigerant	R407C	
Number of refrigerant circuits	Minimum 2 (two)	
Compressor:	Minimum 2 (two)	
Filter	To be mentioned	
Controller	a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
	b) Controller based Sequencing Facility c) water leak detector	
	c) Auto Shutdown by external fire alarm	
	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	

RESTRICTED

Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen, Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

25. Precision Air Conditioner (PAC)_DX for MMR & Power Room		
Description	Required Specification	Bidder's Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 14.8 kW	
Total sensible capacity	Minimum 12.9 kW	

RESTRICTED

Net Capacity	Total	Minimum 14.1 kW	
Net Capacity	Sensible	Minimum 12.2 kW	
Air Flow (Indoor)		Minimum 3,600 m ³ /h	
Air Flow(outdoor)		Minimum 10,600 m ³ /h	
Ambient Temperature		42 °C	
Fan Technology		EC Fan Technology	
Electrical power consumption		Maximum 3.6 kW/Compressor.	
Energy Efficient Ratio (EER)		3.44 kw /better	
Total power consumption		Maximum 4.3 kW	
LpA (2m free field)		Indoor: 56.2 dB(A)	
LpA (5m free field):		Outdoor: 51.1 dB(A)	
Return air temperature		24-26 degree Celsius	
Supply air temperature		14-16 degree Celsius	
Return air relative humidity		50%	
Altitude above sea level:		100 m	
Fan type:		To be mentioned	
Number of Fan		Minimum 1 (one)	
Heat rejection		18.6 kw (per compressor)	
Condenser capacity		18.6 kw each condenser	
Compressor type		Scroll Type	
Expansion Valve		Electronic	
Electrical Heating		9 to 18 kw or more	
Steam humidification		8 to 15 kg	
Refrigerant		R407C	
Number of refrigerant circuits		Minimum 1 (one)	
Compressor:		Minimum 1 (one)	
Filter		To be mentioned	
Controller		a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
		b) Controller based Sequencing Facility c) water leak detector	
		c) Auto Shutdown by external fire alarm	

RESTRICTED

	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	
Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen, Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

26. Chiller		
Description	Required Specification	Bidder's Response
Chiller	<p>The Chiller is an air-cooled, high-efficiency range designed for industrial cooling, IT, and comfort applications that require intensive, year-round use (24/7/365).</p> <p>The entire range is equipped with micro-channel condensers, shell-and-tube evaporators, semi-hermetic screw compressors with capacity slides, low GWP R513A refrigerant, electronic expansion valves, and axial fans with phase-cut modulation or EC brushless technology. It also includes SEC.blue electronic control. All chillers are available in Free Cooling and/or Low Noise versions.</p>	

RESTRICTED

Brand:	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Country of Shipment:	To be mentioned	
Bearing structure	The chiller is manufactured with a bearing structure made of painted galvanized steel profiles assembled with A2 stainless steel small ironmongery. To ensure proper solidity and corrosion resistance, all metal components are made of structural steel complying with UNI EN 10346, with DX51D-type steel and Z200-type coating.	
Electrical cabinet	Electrical cabinet installed on the short side of the chiller, with components and construction in accordance with European regulations CEI EN 60204-1, CEI EN 61000-6-2/4 and EMC 2014/30/UE. Triple leaf metal frame with lock and "double-bit 3-5" key, IP44 degree of protection for outdoor installation	
Refrigerant	The chiller use R513A not flammable refrigerant gas ensuring low environmental impact, no ozone damage (ODP = 0) and a reduced Global Warming Potential (GWP = 573).	
General		
Cooling capacity:	Minimum 260 KW by 2Unit	
EER:	2.91 KW/ better	
Total absorbed Electrical power:	Maximum 67 KW	
S.E.P.R.	5.73	
Ambient temperature working limits	min -10 max 48 °C	
Application	Outdoor	
Outlet water temperature working limits	min 0 max 15 °C	
Refrigerant:	R513A	
Main power supply:	400V/3/50 (V/Ph/Hz)	
Secondaries voltage	230 Vac	
Absorbed electrical power (FLI)	Maximum 106.2 KW	
Absorbed current	Maximum 183.6 A	

RESTRICTED

(FLA)		
Inrush current (MIC)	Maximum 444.6 A	
COMPRESSORS		
Compressor type	Screw	
Number of Compressor	Minimum 1(one)	
Number of refrigerant circuits	Minimum 1(one)	
Absorbed Electrical power	Maximum 61 KW	
Absorbed electrical power (FLI)	Maximum 93 KW	
Absorbed current (FLA)	Maximum 162 A	
FANS		
Fan	3 x ø910	
Fans type	EC	
Air temperature	35 °C	
Fans part load	100%	
Fan air flow	Minimum 90,231 m ³ /h	
Absorbed power at working point	Maximum 7.65 KW	
Max absorbed electrical power (FLI)	0 KW	
Absorbed current (FLA)	Maximum 11.7 A	
HYDRAULIC		
Chilled fluid	Water	
Fluid freezing temperature	0 °C	
Max working pressure	PN 10	
Chilled fluid inlet temp.	12 °C	
Chilled fluid outlet temp.	7 °C	
Fluid flow rate	33.6 m ³ /h	
Pressure drop	49.6 kPa	
Head pressure available	211.1 kPa	
Chilled fluid flow rate	Minimum 24.2 m ³ /h	
Chilled fluid flow rate	Maximum 55 m ³ /h	

RESTRICTED

Width x Height x Depth	4330 x 2485 x 1140 mm	
Weight empty	0 Kg	
Hydraulic connections	3 " M Vic	
Sound pressure level	Maximum 57.5 dB(A)	
Sound power level	Maximum 89.5 dB(A)	
The chillers designed and manufactured in compliance with the EC directive and the EN safety regulations listed below:		
	UNI EN ISO 9001: Quality Management System;	
	UNI EN ISO 14001: Environmental Management;	
	2006/42/EC: Machinery Directive;	
	2014/30/UE: EMC Directive;	
	2014/68/UE: Pressure Equipment Directive;	
	EN 378-1, 2: Refrigerating systems and heat pumps;	
	EN ISO 12100 -1: Safety of machinery;	
	EN ISO 13857: Safety of machinery - Safety distances;	
	EN 60204 -1: Safety of machinery - Electrical equipment;	
	EN 61000-6-2: Immunity for industrial environments;	
	EN 61000-6-4: Emission standard for industrial environments;	
	2009/125/EC: Directive EcoDesign.	
Outdoor installation	All electrical components subject to atmospheric agents have minimum protection degree of IP44	

RESTRICTED

27. Chilled Water (CW) Air Handling Unit for Server Room		
Description	Required Specification	Bidder's Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Water cooled	
Unit configuration Type	Down Flow.	
Total Cooling capacity	Minimum 110.2 kW	
Sensible Cooling capacity	Minimum 110.2 kW	
Net total cooling capacity:	Minimum 103.9 kW	
Net sensible cooling capacity:	Minimum 103.9 kW	
Air Flow (Indoor)	Minimum 27,800 m ³ /h	
Fan Technology	EC Fan Technology	
Total power consumption:	Maximum 6.3 kW	
Energy Efficient Ratio (EER)	17.49 kW/better	
AER	0.23 W/(m ³ /h)	
LpA (2m free field)	61.5 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50 rel.%	
Altitude above sea level:	Minimum 100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 2 (two)	
ESP external static pressure:	20 Pa	
Total pressure drop:	To be mentioned	
Filter	To be mentioned	
2 way-control valve for chilled water control	a) 2-way control ball valve for capacity control of the heat exchanger respectively to control the unit capacity	

RESTRICTED

	b) continuously variable by 0-10V control signal from the controller of the A/C unit	
	c) valve can be manually operated in case of emergency.	
	d) one control valve per circuit	
	e) valve size, valve type, internal valve structure optimized on stable control properties in full load and part load operation	
Dimension (H x W x D):	To be mentioned	
Weight:	To be mentioned	
Voltage	400V/50Hz/3Ph/N/PE	
Electric cabinet/Electrics :		
	Electric cabinet (electric box) integrated in the A/C unit for accommodation of all high voltage and control components; design according to EN 60204-1; protection class: IP20	
	Located in upper front area of the unit; accessible for maintenance exclusively from the front	
	Clear and space saving structure of all high voltage and control components	
	Consistent separation of high voltage and control elements to avoid EMC interferences. This improves the resistance against electro-magnetic noise.	
	All three-phase consumers protected against overload and short circuit by circuit breakers according to IEC/EN 60947-1	
	Completed wiring of motor circuit breakers, contactors and control components in wiring ducts	
	Top hat rail or busbar system for high voltage components	
	Installed main switch (3 poles) operable from the outside, design as load disconnecter	
Installation and Commissioning	Installation and Commissioning should be done by OEM certified Engineer.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	

RESTRICTED

	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

28. Chilled Water (CW) Air Handling Unit for MMR & Power Room		
Description	Required Specification	Bidder's Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Water cooled	
Unit configuration Type	Down Flow.	
Total Cooling capacity	Minimum 16 kW	
Sensible Cooling capacity	Minimum 16 kW	
Net total cooling capacity:	Minimum 15.2 kW	
Net sensible cooling capacity:	Minimum 15.2 kW	
Air Flow (Indoor)	Minimum 4,500 m ³ /h	
Fan Technology	EC Fan Technology	
Total power consumption:	Maximum 0.8 kW	
Energy Efficient Ratio (EER)	20.00 kW/better	
AER	0.18 W/(m ³ /h)	
LpA (2m free field)	53.1 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50 rel.%	
Altitude above sea level:	Minimum 100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 1 (one)	
ESP external static pressure:	20 Pa	
Total pressure drop:	To be mentioned	

RESTRICTED

Filter	To be mentioned	
2 way-control valve for chilled water control	a) 2-way control ball valve for capacity control of the heat exchanger respectively to control the unit capacity	
	b) continuously variable by 0-10V control signal from the controller of the A/C unit	
	c) valve can be manually operated in case of emergency.	
	d) one control valve per circuit	
	e) valve size, valve type, internal valve structure optimized on stable control properties in full load and part load operation	
Dimension (H x W x D):	To be mentioned	
Weight:	To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Electric cabinet/Electrics :		
	Electric cabinet (electric box) integrated in the A/C unit for accommodation of all high voltage and control components; design according to EN 60204-1; protection class: IP20	
	Located in upper front area of the unit; accessible for maintenance exclusively from the front	
	Clear and space saving structure of all high voltage and control components	
	Consistent separation of high voltage and control elements to avoid EMC interferences. This improves the resistance against electro-magnetic noise.	
	All three-phase consumers protected against overload and short circuit by circuit breakers according to IEC/EN 60947-1	
	Completed wiring of motor circuit breakers, contactors and control components in wiring ducts	
	Top hat rail or busbar system for high voltage components	
	Installed main switch (3 poles) operable from the outside, design as load disconnecter	
Installation and Commissioning	Installation and Commissioning should be done by OEM certified Engineer.	
Installation accessories	Required All installation accessories	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor	

RESTRICTED

availability	should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

29. Comfort Cooling (VRF for SOC, NOC, Staggering room & Office area with corridor		
Description	Required Specification	Bidder's Response
Brand	To be mentioned (Preferably Daikin or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of manufacturer	As per Tender Specification Article no 20	
General requirement	Bidder will offer advanced VRF system considering cooling space in SOC, NOC, Staggering room & Office area with corridor as per drawing	
Working hour	Working hour 24X7X365	
Redundant component	The system should be design so that all component should have redundancy & there should be no single point of failure in the operation	
Redundant unit in rooms	<ol style="list-style-type: none"> 1. NOC 2. SOC 3. Tanning room 4. Corridor 	
Outdoor redundancy	Out door should be design so that at least in any out door failure the total cooling capacity should not be decrease.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

30. VESDA System (Very Early Smoke Detection Aspirating) for DC Server, MMR & Power Room with Uptime compliance Zone separation		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Honeywell / Eaton / Xtralis / Bosch / Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Require Features		
Capacity	The proposed solution should be for Approx 6,000 sqft. Floor space.	
	The total electric load will be calculated for 36Racks where each Rack will consist of 5KW load (avg.)	
Additional equipment	Control panels.	
	Releasing devices	
	Remote manual pull stations	
	Corner pulleys	
	Door closures	
	Pressure trips	
	Bells and alarms	
	Pneumatic switches	
	Good to have TCP/IP base remote control capability from Day 1.	
Fire Detection System	Automatic detection for early warning of fire.	
	Should be able to identify different types of smoke.	
	Smoke detectors for gas discharge.	
	The detection circuits should be configured using coincidence or independent inputs.	
Other	If any other components have to be added to design and install the solution To be mentioned and quote the same.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

31. Automated Fire Suppression System for CDC Server, MMR, Battery & Power

RESTRICTED

Room		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Name of the GAS agent	NOVEC-1230	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
General Features	<p>a.The automatic fire suppression system design shall be strictly as per NFPA standard.</p> <p>b.It should be a Clean Agent Gas Based Automatic Fire Suppression System.</p> <p>c.The Seamless storage cylinder shall be for fire suppression system.</p> <p>d.The Valve operating actuators shall be of Electric (Solenoid) type. The actuators should be capable of being functionally tested for periodic servicing requirements.</p> <p>e.The individual cylinder bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure. This mechanism should be integrated as part of the actuator.</p> <p>f.The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.</p> <p>g.The detection and control system that shall be used to trigger the suppression shall employ cross zoning of smoke detectors. A single detector in one zone activated, shall cause an alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.</p> <p>h.The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc.</p> <p>i.The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's patented and certified software.</p> <p>j.Manual Gas Discharge stations and</p> <p>k.Manual Abort Stations shall be provided</p> <p>l.Manual Gas Discharge stations and</p>	
	Bidder will propose solution as per drawing & requirement.	
Refill	The system should be easily refillable	
Refill Support	The proposed Gas should be refillable up to year	

RESTRICTED

	2035.	
	Proper document should be provided to support the time line 2035.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

32. Fire Hydrant System		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Floor to be covered	Bidder will propose as per design & requirement.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

33. Portable fire extinguisher ABC Dry Powder		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Material	ABC Dry Powder	
Weight	10Kg each	
Wall hanging kit	To be provided from day one.	
Powder life time	Should be 2years or above.	

RESTRICTED

Accessories	If any accessories required necessary should be provided.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

34. Portable fire extinguisher CO₂

Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Material	CO ₂	
Weight	5Litter each	
Wall hanging kit	To be provided from day one.	
Powder life time	Should be 2years or above.	
Accessories	If any accessories required necessary should be provided.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

35. Access Control with visitor management System [Quantity: 1 Set (Combination of IRIS (1unit), RFID & Biometric (30 unit) including 31 unit Exit Reader)]

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell or Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20 and South Korea	
Country of Manufacture	As per Tender Specification Article no 20 All the active components quoted for Access control system must be from a single OEM	
ACCESS CONTROLLER & Components	ACCESS DOORCONTROLLER UP TO 4 WIEGAND reader support	
	The access controller must be a rail mountable device for use in specific enclosures as well as existing standard 19" racks	
	The controller shall have a modular design with	

RESTRICTED

	downloadable software so that the application program can be easily updated without touching the controller itself	
	Latest integrated 32-bit, 30 Mhz Micro-controller based system architecture;	
	On board Real Time Clock that will adjust itself to leap year computations automatically	
	ACCESS DOORCONTROLLER shall have 8 Relay outputs; 8 Analog Inputs; onboard LCD display 16 Characters	
	16-characters liquid crystal display (LCD), shall display network parameters and actual status like:	
	a. IP address of the controller	
	b. MAC address of the controller	
	c. DHCP on/off	
	d. Status of all the inputs connected to it	
	e. Status of all the outputs connected to it	
	f. Online and Offline status of the controller	
	g. Firmware version	
	ACCESS DOORCONTROLLER shall include a standard 2GB Compact flash (CF) memory card for storing cardholder data and access events.	
	Memory shall store database that has a capacity with a minimum of 80,000 cardholders and Event buffer size: maximum of 4,00,000 events with date and time stamp.	
	The access controller is UL 294, CE approved.	
	ACCESS DOORCONTROLLER housing shall be in accordance with UL 294 approved and is used for securely mounting and housing the Access Controller, extensions and the power supplies	
	Power supply with battery charger for ACCESS DOORCONTROLLER Shall be with Selectable 12 VDC or 24 VDC voltage output Overvoltage protection Regulates battery charging voltage The product is classified in accordance with the following standards: <ul style="list-style-type: none"> • EN 55022 Class B • EN 55024 • IEC / UL / EN 60950 & CSA (product safety) • CE The Power supply can be mounted on rails and installed in the housing	
Biometric Smart Card Reader	The Finger-print biometric reader provided shall be of ruggedized design, having weatherized polycarbonate enclosure or similar protection to withstand harsh environments for both indoor/outdoor used and provides a high degree of vandal resistance with surface mounting style 13.56 MHz Biometric smart card	

	<p>Reader readers as per tender specifications</p> <p>Biometric readers shall have CPU: ARM® CortexTM-A9 core 1GHz</p> <p>Biometric reader shall be with FBI PIV IQS certified optical fingerprint sensor</p> <p>Operating conditions: Temperature: -20°C to 55°C (-4°F to 131°F) – Humidity: 10% to 80% (non condensing)</p> <p>Ingress protection: IP65</p> <p>Shall have 500 user capacity with expansion capacity of upto 10,000 users</p> <p>Accuracy shall be maintained regardless of number of users in database</p> <p>Biometric reader shall be with 2.8” QVGA color touchscreen and buzzer</p> <p>The specifier shall supply and install the necessary software to manage the Finger-print enrollment for all users and configuration of the Finger-print access control operations. The software provided shall be integrated to the Access Control System for access control and monitoring.</p>	
<p>Smart Reader</p> <p>Card</p>	<p>The Contact less Smart card reader shall provide authentication by reading the Card ID & controller will compare with database and actuating the barrier/turnstile.</p> <p>Contactless smart card readers shall comply with ISO 15693 and shall read credentials that comply with these standards</p> <p>It shall be plug & Play type with suitable locking devices.</p> <p>It shall operate on its own. No software control is required for configuring the threshold sensitivity for readers</p> <p>It shall be possible to exchange the smart card reader without needing to reprogram the control unit</p> <p>The fault of /at one smart card reader shall not affect the functioning of other smart card readers on the network.</p> <p>The readers shall be powered by field panels itself. No external power supply should be used for powering the reader</p> <p>The Card reader shall confirm to ISO 14443</p> <p>The Card reader shall be capable of reading the selected card technologies. (HID iClass/MiFareDESFire EV1 within the 14.56 MHz range).</p> <p>Shall use 64-bit authentication keys to reduce the risk of compromised data or duplicate cards. The contactless smart card reader and cards shall require matching keys in order to function together. All RF data transmission between the card and the reader</p>	

RESTRICTED

	<p>shall be encrypted, using a secure algorithm. It shall have a read range of 5 cm – 7.5 cm when used with the accepted compatible access card technology It shall be capable of providing a unique tone and/or tone sequences for various status conditions such as access granted, access denied, reader power up, etc., and clear visual status LED indication (multi color) shall be provided for various status conditions.</p>	
	<p>Enhanced & optimized multi-tag inventory algorithm with the reading speed of more than 100 tags per second. Built-in 9dBi circular polarized antenna to read an RFID tag in any orientation from vehicle's windshield Supports INDIA 865~867 MHz, EU 865~868MHz, US 902~928MHz working frequency Reliable read distance of up to 12 meters with IDCUBE's specialized ASSA series of long-range credentials Support EPC Global UHF class 1 gen2 / ISO18000-6C protocol RFID tags Integrates with Wiegand/RS232 compatible controllers Support for command, polling and trigger mode</p>	
Smart Cards	iCLASS Seos Contactless Smart Card, 8K memory	
	AES-128/2TDEA cryptographic algorithms for data protection Mutual authentication protocol with generation of diversified session key to protect each card session (using secure messaging)	
	Supports ISO/IEC standards: 7810, 7816 and contactless cards (14443 A)	
	Operating Temperature: - -40 to 70 degrees C and Operating Humidity 5% to 95% relative humidity non-condensing	
Access Control Software	The Access Control System shall have a multi-level priority interrupt structure proven in multi-tasking and multi-client real time applications. Simultaneous alarms/events monitoring by multiple users, system supervision and history archiving shall be possible without degradation of any functionality specified for system or operation.	
	The Access Control System server shall act as the source that provides time synchronization across all sub-systems.	
	<p>The Access Control System shall be capable to support to the following with additional expansion licenses if required:</p> <ul style="list-style-type: none"> • Number of active cardholders – 400,000 • Number of readers – 10,000 • Number of access groups – 255 • Number of time schedules – 255 • 4 – 8 digits programmable (Personal Identification 	

RESTRICTED

	<p>Number) PIN codes</p> <ul style="list-style-type: none"> • Remote Online Locks – 1,000 • Map viewer floor plans – 1,000 	
	<p>Operating Environment: The system server shall be use latest edition of Windows Server 2016 / 2019 and Client shall support Windows 10 shall include network capability with the TCP/IP data communications network protocol and hardware</p>	
	<p>Graphical User Interface: The system shall be a flexible and user-friendly workstation providing user(s) with a Graphical User Interfaces (GUIs) for alarm monitoring and control that includes map viewer with alarm list and a swipe ticker for visual door monitoring. The Access Control System GUI shall support single or multi screen displays having multiple dialogs separately. In case of alarms, the map will automatically focus on the alarm location.</p>	
	<p>Map Viewer and device overview: The system shall contain a map viewer. This map viewer shall provide a graphical presentation of the premises by means of floor plans, pictures or any desired graphical representation. On the maps entrances and devices like MAC, AMC, readers and digital input/outputs can be positioned as a dynamic icons. These graphical icons will display the location of the device in the map and the actual status of the device. Every icon can be displayed in several sizes, angle and color and background color. Clicking any of the devices automatically shows the commands available for controlling the respective device. Control commands are automatically linked based on device type. An operator can be assigned one or multiple authorizations for parts of the map viewer, such as door commands, reader commands, controller commands, system commands, special door commands, digital output commands, alarm list commands, swipe ticker commands. An area overview shall be able to show name, type (e.g. parking), current count, maximum count and state (e.g. empty, full). The ACS System must provide a real-time device overview of the entire system's status. All connected devices are shown on a status tree. A direct control into subsystems is possible by clicking on panel/detector address. A device tree and the device names shall be provided for in the GUI.</p>	

RESTRICTED

	<p>Import Export tool: The Access Control System AS shall provide a web based import and export interface to import cardholder master records from a separate database during installation, or to export the master records for further use by another application in CSV format.</p>	
	<p>Areas The Access Control System shall provide the ability to define and manage arbitrary logical areas within the premises. These could be single rooms, groups of rooms, entire floors or parking areas.</p>	
	<p>Access Sequence Check There shall be an access sequence check provided, allowing authorized cardholders to enter an area only when they have swiped their card at the neighboring area.</p>	
	<p>Threat Level Management: At least 15 different threat levels can be pre-configured for instant activation in case of emergency. A threat level is activated by a threat alert. A threat alert can be triggered in one of the following ways:</p> <ul style="list-style-type: none"> • By a command in the software user interface • By an input signal defined on a local access controller, for instance from a push button or a fire panel. • By swiping an Alert card at a reader <p>Threat alerts can be cancelled by the UI command or hardware signal, but not by alert card.</p>	
	<p>Swipe Ticker: An application can be configured within the Map view that displays the last 10 minutes of access events in a dynamic scrolling list. The operator can easily pause and resume the display. Each record in the list contains details of the event and the credential used, for example:</p> <ul style="list-style-type: none"> • The name of the cardholder and their stored photo, for visual confirmation of identity. • A time stamp. • Company and/or department name • The entrance and the reader at which the credential was used • An event category: Green- Access event Yellow- Incomplete access Red- Invalid access 	
	<p>Random screening: The Access Control System shall be able to perform an additional security check by the officer on duty. The readers are easily set to random screening mode by checking a checkbox and setting the frequency. If the randomizer selects this cardholder for extra</p>	

	<p>security checks. The card is blocked throughout the whole system, until the block is manually removed. Once the screening is done, security can unblock the card or card can be unblocked after certain pre configured time.</p>	
	<p>Blocking cards: The Access Control System shall allow the blocking of cardholders as configured in the system, for example a defined validity period.</p>	
	<p>Alarm Handling and Management: The Access Control System AS shall provide a wide range of standard events. The following events, but not limited to, shall be supported:</p> <ul style="list-style-type: none"> • Card unknown • Card not authorized • Card outside time profile • Card anti-passback • Access timeout • Door open time exceeded • Door opened unauthorized • Door blocked • Tamper alarm controller • Tamper alarm reader • PIN code error • Duress alarm code • Access denied • Wrong card version • Card blocked • Card blacklisted • Card out route • Guard tour alarms • Random screening • Other individual alarm extensions <p>The Access Control System shall provide a wide range of standard events. All events are pre-configured in 4 alarm groups “hold-up”, “alarm”, “warning”, “maintenance”. The incoming alarm or event message shall provide, but not limited to, the following information:</p> <ul style="list-style-type: none"> •Alarm date and time •Alarm status •Alarm location <p>The Access Control System shall provide the operator a simple and efficient way to handle any incoming alarms. The operator shall be allowed to switch between all alarms or events messages. The Access Control System operator shall also be able to send remote commands or activate controls manually from the workstation when requested.</p>	

RESTRICTED

Accessories	Should be mention and quoted as per requirement	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

36. Baggage scanner		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Astrophysics / Garret/Boon Edam / Turn Star / Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Atomic Number Measurement	The Machine must have facility to measure the Atomic Number	
Generator Voltage	Generator Voltage 180kV	
Tunnel Opening - (W x H)	53.3cm x35.8cm	
Max Conveyor Load (kg, lbs)	Approx 165 kg	
Steel Penetration (mm)	Steel Penetration (mm) shall be 39 Typical / 37 Standard	
Wire Resolution (AWG)	Wire Resolution must be (AWG) 40 Typical / 38 Standard	
Centered Image	The machine Shall have Centered Image	
Color Imaging (No black / white)	The Machine must have 6 Color Imaging	
Geometric Image Dist. Correction	The machine Shall have Geometric Image Dist. Correction	
High Penetration	Geometric Image Dist. Correction High Penetration	
Image Annotation	The Machine must have Image Annotation facility	
Material Separation	Material Separation minimum 6	
Nine Quadrant Zoom	The machine Shall have Nine Quadrant Zoom	
Non-Pixel Distortion in Zoom	The Machine must have Non-Pixel Distortion in Zoom facility	
Organic /	The Machine shall be identify Organic / Inorganic	

RESTRICTED

Inorganic Imaging	Imaging	
Picture Clarity	Picture Perfect	
Real Time Image Manipulation	The machine shall have Real Time Image facility	
Continuous Zoom	Continuous Zoom up to 64x	
Display resolution	Display resolution shall be 1280 x 1024 / 24 bit	
Flat LCD Display Monitor	Flat LCD Display Monitor	
Monitor	The Machine must have 19" LCD Monitors	
Operating system	Operating system must be the Windows 10	
PC Processor	Intel® Core i5, 3.1 GHz, 6MB cache	
USB 2.0 Peripherals	USB 2.0 Peripherals Compatible	
USB Memory Stick	USB Memory Stick use ability	
Baggage Counter	Baggage Counter facility	
Computer Based Training (CBT) Lite	Computer Based Training (CBT) Lite	
Continuous Diagnostics	The Machine must have Self Continuous Diagnostics capable	
Continuous Scanning	The Machine must capable Continuous Scanning	
Image Archiving	Image Archiving must be Automatic	
Printer Attachment	The machine shall be capable to connect external Printer	
Save Image RGB (color image)	The Machine must be capable to Save Image RGB (color image)	
TCP/IP	TCP/IP	
User ID Log-in	User ID Log-in	
Emergency Stops	Emergency Stops facility	
Humidity Monitoring	The System must be capable to monitor Humidity	
Read Input Voltage	The System must be capable Read Input Voltage	
Read UPS Capacity	The System must be capable Read UPS Capacity	
Remote Diagnostics	The system must be capable to Remote Diagnostics	
Temperature Monitoring	The system must be capable to Temperature Monitoring	
Built-In UPS	Yes	
X-Ray Self Tuning	Yes	
External UPS for Hole Machine(Optional)	3KVA	
Manufacturer shall have ISO Certificate	Manufacturer shall have ISO Certificate	

RESTRICTED

Machine have TC Certificate	Machine shall have TC Certificate	
Machine have CE Certificate	Machine shall have CE Certificate	
STAC Certificate	Machine shall have STAC Certificate	
TSA Certificate	Machine shall have TSA Certificate	
The Machine Should be UL Standard	The Machine shall be UL Standard	
Included: Entry Exit Rollers	Included: Entry Exit Rollers	
Accessories	Should be mention and quoted as per requirement	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

37. Turnstile Gate with RFID Access control Module		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably TURNSTILES.us /ZKTeco USA/Astrophysics / Garret/Boon Edam / Turn Star / Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Product Size:	To be mentioned	
Passage Direction:	Single directional/Bi-directional	
Throughput Rate:	20~30p/m	
Reaction time	2.0s	
Power Supply	AC100-240V	
Working Environment:-	10-70 °C	

38. Walk through gate		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Astrophysics / Garret/Boon Edam / Turn Star / Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Detection Zones	33 zones (left, right and center); visual and audible alarms with a built-in dry contact alarm relay	
Multi-Unit Synchronization	Synchronization with wired AC power lines or with manual frequency selection for wireless operation	
Visual Displays	LED zone indicator lights on both panels. Pace lights on entry side only, with intuitive images	
Access Control	Eight-button keypad with numerical codes. Keypad lock to control access and to enable/disable the keypad.	
Passageway Interior Size	Width 30" (0.76 m) Height 80" (2.03 m) Depth 23" (0.58 m)	
Overall Exterior Size	Width 35.5" (0.90 m) Height 91.5" (2.32 m)	

RESTRICTED

	Depth 6.25" (.16 m)	
Operating Temperatures	-4° F (-20° C) to +149° F (65° C); Humidity to 95% non-condensing.	
Power	Fully automatic 100 to 240 VAC, 50 or 60 Hertz, 45 watts; no rewiring, switching or adjustments needed	
Regulatory Information	Meets international airport standards such as TSA, ECAC, STAC, AENA, CJIAC, DFT. Meets additional standards and requirements such as USMS, NIJ-0601.02, NILECJ. Meets Electrical Safety and Compatibility Requirements for CE, FCC, CSA, IEC, ICNIRP, IEEE.	
Weatherproofing	Meets IP 55, IP 65, IEC 529 Standard for moisture, foreign matter protection	
Construction	Attractive scratch and mar-resistant laminate. Detection Heads and Support: heavy duty aluminium.	
Control Outputs	Solid state switches (low voltage AC or DC) for operating external alarms and control devices	

39. CCTV Surveillance System		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell or Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
	All the active components quoted for Access control system must be from a single OEM	
Physical Dimension	Please Mention	
NDAA compliant	Should be NDAA Compliant	
Resolution	Minimum 5 MP	
Image sensor type	Should have 1/2.7"	
Max. frames per second (fps)	Minimum 30@5MP	
Indoor / outdoor	Outdoor	
Quantity	a). Bullet IP Camera-40Nos b). PTZ IP Camera-10Nos c). Dome IP Camera-14Nos	
Built-in IR lighting	Should have 30 Meter / 98 Feet	
Wide Dynamic Range	Should have 120db	

RESTRICTED

ONVIF conformant	Should be ONVIF Conformant	
Power over Ethernet (PoE / PoE+)	Should have PoE Port	
Advanced Features		
Compression	Should have H.265, H.264, MJPEG	
Multi-streaming	Should have 3 streams	
Intelligent Dynamic Noise Reduction	Should have Intelligent Dynamic Noise Reduction	
Intelligent streaming	Should have Intelligent streaming	
Alarm triggering		
Video Analytics - pre-installed	Should ve IVA Pro Buildings	
Tamper detection	Should have temper detection	
Sensitivity		
Min. illumination day mode (color)	Should be 0.14 lux	
Min. Illumination night mode (B/W)	Should be 0 lux	
Lens		
Varifocal	Should be varifocal	
Automatic Varifocal (AVF)	Should be Automatic Varifocal (AVF)	
Iris control	Should have DC-iris	
Focal length from	Minimum 3.3 mm / 1.30 Inch	
Focal length till	Minimum 10.2 mm / 4.02 Inch	
Horizontal Angle of View (HAoV)	Minimum 30.1° x 101.4°	
Min. view angle (H)	Minimum 30.1°	
Min. view angle (V)	Minimum 21.8°	
Max. view angle (H)	Minimum 101.4°	
Max. view angle (V)	Minimum 69.6°	
Tilt angle	Minimum 0~85	
DCRI distances (in m with 100 lux illumination)		
Detection	Minimum 42m-193m	
Classification	Minimum 17m-77m	
Recognition	Minimum 9m-39m	
Identification	Minimum 4m-19m	
Storage		

RESTRICTED

(micro)SD-card slot	Should have (micro)SD-card slot	
Capacity of SD Card	Should have 64GB micro SD card in each camera from day one.	
Direct-to-iSCSI	Should able to connect with direct-to-iSCSI	
Housing		
Weather rating	IP66	
Vandal resistant	IK10	
Operating temperature	-30C to 50C (-22F to 122F)	
Network Video Recorder		
Processor	Quantity-02 Minimum Intel Xeon Processor E3-1275 V3 (8 MB Cache, 3.5 GHz) processor	
Cache	Minimum 8 MB Intel Smart Cache	
Memory	Minimum 8 GB, DDR3-1666 ECC UNB (1 x 8 GB)	
HDD slots	Minimum 16 slots, 3.5 in. SATA storage trays	
HDD for video	Minimum 8TB/HDD Total Number of HDD 16Nos.	
SSD for OS	Minimum 2 x 120 GB SSD drives in RAID-1 configuration	
OS	Should have Windows Storage Server 2012 R2 license built in	
RAID support	Should support RAID-5 / 6	
Protocol	Should be iSCSI	
B/W capacity	Minimum 550 Mbit/s	
Network	Should have dual Gigabit LAN (teamed)	
Hot swappable HDDs	Yes	
Hot swappable power supply, fans	Yes	
65" LED Display for CCTV view.	2Nos	
Power Consumption	Please mention	
Power Input	Please mention	
Form Factor	Should be rack mountable. Please mention	
USB Ports	Should have Front: 2 USB 2.0 ports, Rear: 2 USB 2.0 ports, 2 USB 3.0 ports	
Dimensions (H x W x D)	Please mention	
Weight	Please mention	
Operating Temperature	Please mention	
Non-operating Temperature	Please mention	
Operating	Please mention	

RESTRICTED

Relative Humidity		
Non-operating Relative Humidity	Please mention	
Quality	This product shall be manufactured by a firm whose quality system is in compliance with the I.S. /ISO 9001/EN 29001, QUALITY SYSTEM.	
SNMP	Should support Simple Network Management Protocol is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.	

40. Raised Floor		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Arctiv/ RHGx600/ Maro or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Total Floor Area	Approx. 6,000sft. (Bidder will proposed as per drawing & requirement)	
Features of Solid Panel	1.Fiber-reinforced Calcium Sulphate Panel	
	2.Panel thickness: 32 mm minimum	
	3.High pressure laminate: 1.0mm HPL minimum	
	4.Uniform Load: 23000N/m ²	
	5.Point Load/Concentrated load: 450KG	
	6.Rolling Load: 4450N/10 times	
	7.Panel Weight: 18 KG approx	
	8.Concentrated Load: 450 KG	
	9.The panel shall meet the high requirements regarding dimensional accuracy acc. to RAL-GZ 941/EN12825 to guarantee high air tightness. High air leakage rate requirements are guaranteed as well.	

RESTRICTED

	10.Panel should be fire proof, dustproof and corrosion resistant	
	11.Panel size: 600 x 600 mm	
	12.Accessories: Pedistal, stringer, gasket etc.	
	13.Raised floor panels/tiles must be Anti-static with 1.5 Ft. high steel understructure.	
	14.The legs of the raised floor are all separate from each other	
	15.All legs of the raised floor are connected with earthing cable.	
	16.To pass the electric cable from the rack to the power socket under the raised floor proper cap to be used in the raised floor tiles.	
	17.The raised floor should be installed in such a way that the PAC for down flow and the proposed water detection system can be installed properly and can be serviced easily afterward.	
Features of Perforated Panel	1.Perforated steel panels designed for static load shall be interchangeable with standard field panels and capable of supporting concentrated loads with at least the load carrying capacity as the standard panels.	
	2.Panels shall have 58% or higher free air flow with Damper	
	3.Panel shall have damper added to control the airflow (optional)	
	4.The panel carrier plate consisting of a welded tube frame and must be conductive powder coated	
	5.Panel should made of non combustible materials	
	6.Panel size: 600 x 600 mm	
	7.Panel thickness: 32 mm minimum	
	8.Concentrate load: 3650N	
	9Load bearing capacity: 16,100 N/m ²	
	10.Accessories: Pedistal, stringer, gasket etc.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	

Warranty	Three (03) years full warranty	
----------	--------------------------------	--

a

41. Data Center Floor insulation		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Total Floor area	Approx. 6,000sft. (Bidder will proposed as per drawing & requirement)	
Features	a. A closed- cell structure not prone to wicking b. Mould resistance c. Dust and fiber-free construction d. An in- built water vapour barrier e. Ease of cutting and fitting f. Durability and maintenance	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

42. Dry wall & Paint Works		
Feature List	Feature Description	Bidder Response
Dry wall	Fire rated two layer Gypsum Board Partition	
	10" Thickness two layer Gypsum board partition work with first class fire rated gypsum board. Inside the board should use glass wool to protect fire. MS Metal frame with all necessary accessories.	
Total area	Bidder will proposed as per drawing & requirement	
Paint work	Epoxy paint for inside server room, power room wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: To be mentioned	
	Country of manufacture: To be mentioned	
	Approved colour of epoxy paint to wall/column of inside wall,of the server room, power room,	

RESTRICTED

	etc of two coats over a coat of brand specified primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding by roller/ spray etc and printing with two coats of epoxy paint approved color over a coat of priming etc all complete as per direction	
	Normal Paint for noc room and other wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: Bangladesh	
	Country of manufacture: Bangladesh	
	approved colour of normal paint to wall/column of inside wall,of the NOC, staging, open area etc of two coats over a coat of brand specified primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding by roller/ spray etc and printing with two coats of normal paint approved color over a coat of priming etc all complete as per direction	

43. Water Leak Detection System to cover Data Center floor (Server, MMR & Power rooms) all critical areas & points) embedded with Monitoring & Notification


Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
General requirement	Water Leak Detection System to cover Data Center floor (Server, MMR & Power rooms) all critical areas & points) embedded with Monitoring & Notification	
Floor area to be covered	Bidder will propose as per design & requirement.	

RESTRICTED

Features	<ul style="list-style-type: none"> a. should be able to detect the moisture bellow the raised floor. b. It should provide immediate warning after detecting the moisture and water. c. It should be Micro-Processor Based Control 	
	<ul style="list-style-type: none"> d. Monitors each zone independently. e. Provides subsequent alarming, no matter how many zones go into ALARM or FAULT. f. Identifies location, time & date of all ALARM and FAULT conditions. g. Alarming should be provided at-least via two or more of the below state method Audible Visual h. In-band and out-of-band methods indicating in the software console and/or in the Building management system. i. Monitoring software should be provided with the system. j. Each cable length should be 20 feet or higher. k. To provide the solution if any other component has to add it should be included and the price should be required. 	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	


44. Lightning Protection System		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of manufacturer	As per Tender Specification Article no 20	
General Features	<ul style="list-style-type: none"> a. A lightning protection system includes a network of air terminals, bonding conductors, and ground electrodes designed to provide a low impedance path to ground for potential strikes. b. Required resistance <1 Ohm c. Grounding rods, inspection pit, lightning event counter have to be considered. 	


45. Rodent System		
Brand	To be mentioned (Preferably Maser or Equivalent)	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Master controller	Bidder will offer advanced rodent repellent system considering as per drawing.	
Transducer	Bidder will offer transducer considering as per drawing.	
Wire bundle	Wire bundle	
Installation	Installation Material, Testing & Commissioning Charge	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

46. NOC with Gallery type seating arrangement		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Specifications of Display Panel	Please Specify	
Number of steps in gallery	02	
Number of seats per steps	04	
LCD panel size of the NOC room	(W:H)(20' X10')	
Number of display for the LCD panel	At least 15nos	
Size of each display for the LCD panel	55" or above (Preferably SAMSUNG) .	
Sample image		
Functionality Required	<ul style="list-style-type: none"> ➤ Linear and asymmetric ➤ Scheduled play ➤ Multiple aspect ratios ➤ Full HD on every screen ➤ Display multiple sources ➤ Display images across single or multiple screens ➤ HDCP support ➤ Image rotation ➤ Art wall (any angle) ➤ Remote monitor management Live camera and PC feeds	
Specifications of Central Server	Please Specify	
Specifications of individual video controller/Set Back Box	Please Specify	
Electrical Network and	All network and power connections (from Bus-bar) have to be provided.	

RESTRICTED


Infrastructure work	All infrastructure work (Brick, tiles, Iron work, interior etc as per attached sample image or vatted by the BNNET acceptance committee .	
Chair	10number of comfortable chair with headrest	
Table	As required for 2 rows, 4person in each row	
Drawer cabinet	At least 8 set.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

47. SOC with seating arrangement		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Specifications of Display Panel	Please Specify	
Number of row in SOC	02	
Number of seats per row	03	
LCD panel size of the NOC room	(W:H)(14' X10')	
Number of display for the LCD panel	At least 9nos	
Size of each display for the LCD panel	55" or above (Preferably SAMSUNG).	
Sample image		

		
Functionality Required	<ul style="list-style-type: none"> ➤ Linear and asymmetric ➤ Scheduled play ➤ Multiple aspect ratios ➤ Full HD on every screen ➤ Display multiple sources ➤ Display images across single or multiple screens ➤ HDCP support ➤ Image rotation ➤ Art wall (any angle) ➤ Remote monitor management <p>Live camera and PC feeds</p>	
Specifications of Central Server	Please Specify	
Specifications of individual video controller/Set Back Box	Please Specify	
Electrical and Network	All network and power connections (from Bus-bar) have to be provided.	
Infrastructure work	All infrastructure work (Brick, tiles, Iron work, interior etc as per attached sample image or vatted by the BNNET acceptance committee .	
Chair	10number of comfortable chair with headrest	
Table	As required for 2 rows, 3person in each row	
Drawer cabinet	At least 6 set.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

48. Fork-lift for equipment Movement inside Data Center		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	

RESTRICTED

Load Capacity	Please Specify (Minm 450KG)	
Lifting Capacity	Please Specify (Minm7 Feet)	
Dimension	Please Specify	
Horizontal extension arm	Minimum 1000 mm	
Sample image		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

49. PA System		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
01X Controller	Public Addressable Voice Alarm System (PAVA)	
	Model/Part Number: Please mention	
	EN 54-16 certified and EN 60849 compliant	
	The controller can be used as a stand-alone system with up to six zones, or expanded to up to 120 zones using additional six-zone routers.	
	Up to eight call stations	
	One-channel or two-channel operation	
	Fully supervised system	
	Heart of the Plena Voice Alarm System	
	Six-zone system controller	
	Built-in 240 W amplifier	
	6 emergency and 6 business triggers	
	Approvals: Europe CE Declaration of Conformity, Poland CNBOP	

RESTRICTED

3 X Zone Call Station for Main amp zone		
	Model/Part Number: Please mention	
	Stylish six-zone call station for the Plena Voice Alarm System	
	Six zone selection keys, all-call key and momentary PTT-key for calls	
	Selectable gain, speech filter, limiter, and output level for improved intelligibility	
	LED indications for zone selection, fault, and emergency state	
	Call station extension provides seven additional zone and zone group keys	
	Approvals: Europe CE Declaration of Conformity	
3 X 07 Zone Plena Voice Alarm Keypad		
	Model/Part Number: Please mention	
	Seven zone selection keys	
	LED indications for zone selection	
	Up to eight keypads can be connected together	
	Approvals: Europe CE Declaration of Conformity	
3 X Power Amplifier for Each Zone (480W)		
	Model/Part Number: Please mention	
	480 W power amplifier in a compact housing	
	70 V / 100 V and 8 ohm outputs	
	The Amplifire Shall have Dual inputs with priority switching	
	100 V input for slave operation on 100 V speaker line	
	The Amplifire shall Temperature controlled forced front to back ventilation, directly stackable.	
	The Amplifire shall have facility Mains, battery back-up and pilot tone supervision	
	Approvals: Europe CE Declaration of Conformity	
Plena Voice Alarm Router	As required	
	Model/Part Number: Please mention	
	Expand the voice alarm system with six zone	
	EN 54-16 certified and EN 60849 compliant	
	12 additional input contacts	
	Six volume override output contacts	
	Supervision within the Plena Voice Alarm System	
	Approvals: Europe CE Declaration of Conformity	
25 X 5W Premium Sound Cabinet Loudspeaker		

RESTRICTED

	Model/Part Number: Please mention	
	High-fidelity music and speech reproduction	
	Selectable 8 ohm, 70 V and 100 V inputs	
	Compact yet robust ABS enclosure	
	Supplied with adjustable mounting bracket	
	Complies with international installation and safety regulations	
	Approvals: Europe CE Declaration of Conformity	
3 X 10 W Horn Loudspeaker		
	Model/Part Number: Please mention	
	Up to 45 W (max. power)	
	Wide opening angle	
	Water- and dust protected to IP 65	
	Versatile mounting bracket	
	Approvals: Europe CE Declaration of Conformity	
PLE-SDT Plena Easy Line SD Tuner BGM source	As required	
	Model/Part Number: Please mention	
	MP3 playback from SD card and USB inputs	
	FM tuner with RDS, presets and digital control	
	Simultaneous operation of SD/USB-player and FM tuner	
	Separate outputs for digital source and FM tuner	
	Approvals: Europe CE Declaration of Conformity	
Fire Detection & PAVA System Integration Device		
	Model/Part Number: Please mention	
	Connection of peripherals with RS232 serial interface	
	Ready to go thanks to plug-and-play technology and pluggable terminal blocks	
	The System shall have facility Seamless Integration between PAVA and Fire Alarm System	
	Approvals: Europe CE Declaration of Conformity	
2X1.5m Cable		
	Brand: BRB/Partex	
	Origin: Bangladesh	
1 X 15U Server Rack	15U Server Rack	
Brand	TO BE MENTIONED	
Model	TO BE MENTIONED	
Origin	TO BE MENTIONED	
PVC pipe with Accessories		
	Brand: Poly/Bengal/RFL	
	Origin: Bangladesh	

RESTRICTED

	20 mm dia PVC pipe with related joints	
Installation	Supply, Installation, Programming, Commissioning of the System	
Instruction and other activities		
As built design	Bidder should provide a built-up design with details during implementation and FAT period	
Labelling	Printed labelling enclosed with each applicable item	
Others	Bidder should accommodate additional items if required during the implementation period.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

50. Wireless Powered Desktop Laminated Label Printer -(Quantity: 2 Set)		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Type	Barcode Label Printer	
Printing Method	Thermal Transfer	
Cutter	Automatic	
Max. Print Speed	60 mm/sec	
Paper/Media Types	TZe, HSe, FLe	
Tape Size	36mm	
Maximum Tape Width	36mm	
Memory	6MB	
Interface (Built-in)	USB, Wi-Fi, Serial	
Cartridge	Bidder will provide at least 50nos cartridge with this label printer.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

RESTRICTED

51. Dual-Sided Card Printer with ribbons & cards.		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Type	Card Printer	
Print Speed (Black)	450cph	
Print Speed (Color)	140cph	
Power Source/ Power Consumption	90-132VAC and 190-264VAC RMS	
Ribbons	20nos of ribbons to be provided in day one.	
Card	100nos of ribbons to be provided in day one.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

52. Fire rated door for data center (Quantity: 6nos Single leaf(3'6"X7'), 1nos double leaf (6'0"X7') , 7nos double leaf (5'0"X7')		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Feature		
Fire rating	for 120 Minutes, Conforms to IS3614 (PART-2)1992, BS476 (PART 20 & 22) and ISO834.	
Material:	Door Frames and Leaves are made from Galvanized Steel	
Door Leaves:	Constructed from 2.0mm thick galvanized steel sheet formed to provide a 48mm thick fully flush, double skin door shell with seamless welding joint all around. The internal construction of the door shall be specially designed with infill to give 2 hours fire rating.	
Infill:	All the doors will have Honey Comb Crafted Paper or equivalent infill.	
Vision panel:	Fire Rated glass vision panel	

RESTRICTED

Accessories	Hinge, bolt and screw: Fire rated lock: Built in mortise lock Auto Door Closer: Default Push panic bar: built in	
Standards	UL Listed Fire door NFPA 251 Standard Test standard: Fire Door must be tested according to BS Standard	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

53. Data Center Design Validation and Tier-3 Certification		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Design validation for Tire 3:	from Uptime Institute/epi/equivalent	
Data Center Certification for Tire 3:	from Uptime Institute/epi/equivalent	
Detailed drawing for Tier-3 design certification from Uptime Institute/epi	Bidder have to comply	
After completion of Data Center vendor has to take necessary measure to get a tier-3 Data Center Certification from Uptime Institute/epi.	Bidder have to comply	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

TENDER SPECIFICATION FOR DRDC PASSIVE EQUIPMENT**Passive Hardware for DRDC**

1. Server Rack with KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/ / Vertiv / Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1500 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	Ø 04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 1U Universal Horizontal Cable Manager	
	Ø 04 units 2U Universal Horizontal Cable Manager	
Vertical Cable Manager	At least 4 Vertical cable managers should be provided with each rack.	
Fixed trays/shelves	2 Fixed trays/shelves capable of caring at least 50 kg load, depth of at least 900 mm should be	

RESTRICTED

	provided with each rack	
Sliding trays/shelves	1 Sliding trays/shelves should be provided with each rack	
Tool less Airflow Management	At least 20 U blank panel should be provided with each rack	
Blanking Panels		
Stabilization	Should be provided	
Rack Monitor	17" TFT rack mount APC/Vertiv/Arctiv or equivalent monitor which occupies only 1 U / 2U rack space 1 unit for each rack	
Integrated Keyboard and Mouse	Required with sliding functionality	
Power Distribution Unit (PDU) with built-in K-type transformer	Switched Rack PDU, 32A – At least 24 way, 02 units: Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads Metered Rack PDU, 32A – At least 42 way, 02 units: Active monitoring and alarms to warn of potential overloads	
KVM Switch	Switch that allows 2 users (one remote & one local User) single-point access and control of up to 16 multiple servers from a single console with 16 units KVM console cable and 16 units 1.5mtr cat 6 & 16 units 3mtr cat 6 patch cord	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each Rack to connect the servers/network/PDU equipment with the quoted rack. 02 units of C20 to industrial female (32A) 02 units of C19 to industrial male (32A) 02 units of C14 to industrial female (16A) 02 units of C13 to industrial male (16A) 04 units of C19 to C20 cable (16A, 3m). 10 units of C13 to C14 cable (10A, 3m). 10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

2. Rack without KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1200 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 1U Universal Horizontal Cable Manager	
	04 units 2U Universal Horizontal Cable Manager	
Tool less Airflow Management	At least 20 U blank panel should be provided with each rack	
Blanking Panels		
Stabilization	Should be provided	
Power Distribution Unit	Metered Rack PDU, 32A – At least 42	

RESTRICTED

(PDU) with built-in K-type transformer	way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
	Switched Rack PDU, 32A– At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.-	
	02 units of C20 to industrial Male (32A)	
	02 units of C19 to industrial Female (32A)	
	12 units of C19 to C20 cable (16A, 3m).	
	10 units of C19 to C20 cable (16A, 2m)	
	10 units of C13 to C14 cable (10A, 3m).	
	10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

3. Hot-aisle Containment System		
Feature List	Feature Description	Bidder Response
Brand name	To be mentioned (Preferably Schneider / Vertiv / Arctiv / Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
No. of Racks	20 Racks	
Ducting Arrangements	There will be 02 types of Precision cooling available at CDC i.e Chiller based and DX based. A common ducting system should be used.	
Containment Specifications	<ul style="list-style-type: none"> a. The Aisle should be sized for two equal length rows & one single aisle of IT enclosures with supporting infrastructure with Top Cable Troughs. b. Hot aisle ducted configuration. c. Ceiling and duct panels must be constructed in a rectangular fashion and 	

RESTRICTED

	<p>extend vertically.</p> <p>d. The Containment uses a series of polycarbonate panels, door frames and doors, and air blocks to enclose a Hot aisle zone which contains cooling unit supply air.</p> <p>e. All system components should be certified as suitable for this data center environment by documentation supporting UL Listings: UL484, CSA C22.2 No.236 and UL723S.</p>	
Duct/AIR RETURN SYSTEM (as per design requirement)	<p>a. Should be 6.0 mm thick Lexan clear-ribbed panels or 2.36 mm thick V0 clear panels with aluminum framing/equivalent.</p> <p>b. Flame spread rates: Smoke development index "0-65" and flame spread index "0" in accordance with UL723 or ASTM84. Nominal thickness: 2.36 mm (V0 clear) –or– Smoke development index "20" and flame spread index "0" in accordance with UL723 or ASTM84. Nominal thickness: 6.0 mm (Lexan)</p> <p>c. Minimum Light Transmission per ASTM D1003 equal to 82% or greater.</p> <p>d. Duct panels should be designed to be supported by the frames of the IT Equipment racks. Ceiling Panel frames sizes should be suitable to match up with various rack widths, row width, and hot aisle widths.</p> <p>e. The air return system should be designed to permit removal of the air blocks from within the contained zone without the use of tools for service access to the space above the Aisle.</p>	
RACK EQUIPMENT BAYING KITS (as per design requirement)	<p>Metal and plastic components should be supplied to establish consistent spacing between the racks or rack-based equipment, and to fill the space to provide an air containment seal at the juncture between two adjacent racks or rack-based equipment.</p>	
DOOR FRAMES AND DOORS (as per design requirement)	<p>a. Door frames and doors shall be provided to establish air containment at the end of two rows of racks. The door frame system shall match the height of the rack based equipment, and match the design width of the contained aisle.</p> <p>b. Materials: Aluminum, SPCC and Tempered Glass.</p>	

RESTRICTED

	<ul style="list-style-type: none"> c. Doors shall be Sliding, to permit access into the contained aisle for maintenance or servicing. d. Doors shall be provided with a window, handles or latches. e. Two proximity switches provided per door for open/closed status f. Electronic Access Control: Smart PIN based,RFID g. LED Lights: Automatic lighting to sync to the automatic doors h. Automatic door closure system for sliding door i. Sliding Doors should be provided with swing-open functionality in case of emergency inside the aisle. 	
<p>FRAMES AND COMPONENTS SEALS (as per design requirement)</p>	<ul style="list-style-type: none"> a. Foam Rubber gaskets or metal/composite, brush, or plastic air blocks should be installed at Aisle joints to minimize open gaps between containment system components, such as door frames, ceiling and duct panels, and IT Equipment racks and rack-based equipment. Gasketing and/or air blocks may include, but not be limited to, the following. b. Joints between adjacent ceiling/duct panels c. Joints between ceiling/duct panels and top of racks, if not metal to metal. d. Joints between door frames and ceiling/duct panels, if not metal to metal. e. Joints between door frames and racks at the end of the row(s). f. Joints between rack bottom rear frame and floor. g. Joints between duct panel and ceiling/roof of room. 	
<p>Air Return System (as per design requirement)</p>	<ul style="list-style-type: none"> a. Should consist of duct mounting rails and duct panels b. Mount to top of racks and extend up to ceiling plenum c. Allows for flexibility with overhead cabling and cable troughs d. Adjustable height supports e. Should support duct structure and extend duct upward to ceiling plenum f. Should mount to top of racks and rack height adapters g. Should be adjusted to be level with ceiling 	

RESTRICTED

	<ul style="list-style-type: none"> h. Should be placed every 600mm apart spanning length of aisle i. Should be provided with mounting bracket for various racks j. Should be provided with removable lexan or V0 airblocks and all necessary hardware to seal gap between top of racks and bottom duct rail k. Should be provided with Modular PDU and/or Rack Mounting brackets if needed 	
<p>Blanking Panels, Height Adapters, and Depth Extenders (as per design requirement)</p>		
	<ul style="list-style-type: none"> a. Blanking Panels should be placed where gaps between racks exist to seal contained aisle. The panel should match the height of the enclosures and match the width of the gap. It should not be mounted to any adjacent blanking panels nor should it support any adjustable height supports. b. Depth Extenders should mount to front or back of enclosures to align aisle. The extender should match the depth of the adjacent racks and match the width and height of the enclosure (including any height adapters) of which it is being mounted c. Height Adapters should mount to the top of enclosures to align the enclosure height. The height adapter match the height of the adjacent racks and should match the width and depth of the rack (including any depth adapters) of which it is being mounted. d. Containment should Prevents short circuiting of cold air with warm air e. Provides even temperature across the cabinet height. f. Containment should Enhances equipment performance by increasing the temperature gradient g. Top Panel should comply to following points: h. Frame work should be CRCA Steel made of (600 mm / 800 mm wide) i. CRCA Steel is as per "IS 513 Grade D" j. Toughened Glass or Polycarbonate 	

RESTRICTED

	<p>panel (Lexan panel)</p> <p>k. Doors (Sliding or Swivel) should comply to following points</p> <p>l. CRCA frame (1.2mm thickness) work and toughened glass (4mm thickness) or Lexan sheet (4mm thick).</p> <p>m. Sliding mechanism or Swivel mechanism with hinges.</p> <p>n. PU Foam Gasket should run across the edges of the door to prevent any leakage of cold air.</p> <p>o. Polyamide Cable Brushes are fitted at the bottom of doors to avoid leakage of cold air when doors are closed.</p> <p>p. All metal components should be power coated with Powder coat is with Nano ceramic pre-treatment process using a zirconium coat.</p>	
	q. The Powder coating process should be ROHS compliant.	
	r. Powder coating thickness shall be 80 to 100 microns.	
	s. Cabinet Rows should be either side of the Hot Aisle to be identical.	
	t. Side Sealing Kits for cabinet to avoid air short cycling.	
	u. Blanking Panels should be for unused "U" spaces.	
	<p>v. Side Panel should be plain i.e. without venting / perforation.</p> <p>w. Top Panels should be plain without Fans.</p> <p>x. Cabinet Front and rear door should be perforated.</p> <p>y. All the racks should be of same height.</p>	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

4. Automatic Voltage Regulator-500KVA		
Feature List	Feature Description	Bidder Response
Brand:	To be mentioned (Preferably Ortea/IREAM or equivalent)	
Model:	To be mentioned	
Country of origin:	As per Tender Specification Article no 20	
Manufacturing Country:	As per Tender Specification Article no 20	
Capacity:	500 KVA	
Input:		
System:	Three Phase	
Input voltage variation:	±15 %	
Input voltage range:	340-460 V	
Frequency:	50Hz ±5% or 60Hz ±5%	
Max input current:	As per design	
Output voltage:	400 V	
Rated output current:	As per design	
Efficiency:	>98 %	
Adjustment speed:	24 ms/V	
Control:	Servo motor	
Standard features		
Voltage stabilization:	Independent phase control	
Admitted load imbalance:	100 %	
Ambient temperature:	-25/+45°C	
Storage temperature:	-25/+60°C	
Max relative humidity:	<95% (non-condensing)	
Admitted overload:	200% 2min.	
Harmonic distortion:	None introduced	
Protection degree:	IP 21	
Overvoltage protection:	Class II output surge arrestors, Optimal voltage return through supercapacitors in case of black-out	
Communication ports	RS232,RS485,Bluetooth, Ethernet, Slot for SNMP	
Remote Monitoring:	SNMP based Remote monitoring capability and compatible with Data Center Infrastructure Management System (DCIM)	
Dimensions WxDxH:	To be mentioned	
Weight:	To be mentioned	
Installation & Commissioning:	Installation, testing and commissioning with necessary accessories.	
MAF	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
BOM	BOM to be attached with technical	

RESTRICTED

	compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

5. Modular Online UPS-150KVA/KW

Feature List	Feature Description	Bidder Response
General Requirement	The vendor shall provide 2x150 KVA modular Hot Swappable UPS in (N+N) configuration. The power cabinet must be of 250 KVA each. Also, each power cabinet shall be consisting of multiple numbers of hot-swappable power modules.	
Brand:	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Country of Shipment:	To be mentioned	
Capacity:	Minimum 150 KVA to be upgradable up to Min 250 KVA in a single cabinet.	
Module:	Each Module will be minimum 25KW Hot Plug and hot swappable function	
Number of Module:	To be mentioned.	
Backup Time:	Minimum 30 min at 150 KW full load from two separate battery Bank Combinedly. Each battery bank shall capable to provide backup for minimum 15 minute at 150 KW full load	
Battery String(Bank):	Each UPS Shall have Minimum two (2) battery String /Bank /Cabinet with separate controller per string/Bank/Cabinet.	
Input Battery Voltage:	Selectable and Configurable	
Topology:	Modular, True Online Double Conversion with Distributed/ Decentralized Active Redundant Architecture	
Input Power factor:	Minimum 0.99 at full load	
Output Power factor:	1 or unity	
Input		
Input Wiring:	3Ph+N+PE	
Rated Voltage:	380/400/415Vac	
Voltage Range:	For loads <100% (-25%, +20%) <80% (-32.5%, +20%) <60% (-35%, +20%)	
Input Frequency:	40-70 Hz	

RESTRICTED

Total Harmonic Distortion:	THDi<3% for linear load, THDi<5% for nonlinear load	
Bypass		
Input Wiring:	3Ph+N+PE	
Rated Voltage:	380/400/415Vac	
Input Frequency:	50/60 ±2/4% (selectable)	
Input Feed:	Duel	
Output		
Output Wiring:	3Ph+N+PE	
Rated Voltage:	380/400/415Vac	
Frequency:	50 Hz / 60 Hz	
Waveform:	Sine wave (THDv<1% for linear load THDv<3% for non-linear load)	
Overload Capacity:	Inverter 124% continuous 125% overload for 10 min 150% overload for 1 min, Bypass 135% overload for long term <1000% overload for 100ms	
Crest factor:	3:01	
General Features		
Features of individual Modules of Modular UPS system:	Individual rectifier, inverter, Control Logic, Static Bypass, On/Off Switch and LCD Display.	
Redundancy, Fault tolerance and Fault Isolation	The UPS System shall Design for no single point of failure and should be driven by the different modules. It will not consist of any major component failure of which may cause the failure of all module's operations. It shall have fault isolation capability. True hot Swappable function.	
Controller:	Separate controller for each module.	
Alarm/Status Indicator	Alarm/Status Indicator for each module.	
Mechanical Bypass:	Central mechanical bypass switch	
Battery Connection:	Please mention	
Supported Battery Type:	Lithium-Ion and VRLA	
Efficiency (VFI):	Minimum 97 %	
Environment		
Protection rating:	IP 20 or Better	
Operating Temperature	0-40°C or To be mentioned	
Relative Humidity	To be mentioned	
Operating Altitude	Minimum 100 m without any derating	
Audible Noise	< 65dB or Better	
Communication		
LCD Display:	UPS shall have Minimum 6 inch (Diagonal) LCD Display for showing all necessary information Centrally. And individual LCD display for each module.	
Communication	RS232,RS485,Bluetooth, Ethernet, Slot for	

RESTRICTED

ports:	SNMP	
Remote Monitoring & Management:	SNMP based Remote monitoring capability and compatible with Data Center Infrastructure Management System (DCIM)	
Standard:		
Safety:	IEC/EN 62040-1	
Electromagnetic Compatibility:	IEC/EN 62040-2	
Performance:	IEC/EN 62040-3	
Manufacturer Certification:	ISO 9001/ ISO 50001	
UPS Cabinet Weight & Dimension:		
Weight:	To be mentioned	
Dimension: WxHxD(mm):	To be mentioned	
Battery Specification		
Battery Type:	Lithium-ion	
Brand:	Please mention	
Model:	To be mentioned	
Country of Origin:	To be mentioned	
Country of Manufacture:	To be mentioned	
Nominal Voltage:	To be mentioned	
Battery Module:	The UPS shall have hot swappable battery module. Can be run with Lower/Higher number of Battery module.	
Battery Amp:	To be mentioned	
Number of Batteries:	To be mentioned	
Weight per Battery (Kg):	To be mentioned	
Battery Dimension:	To be mentioned	
Designed Life Time for Battery:	Minimum 15 Years	
Battery Cabinet:	External type best quality battery cabinet with circuit breaker, Controller with required electrical/electronic components, Battery Monitoring System and shielded battery module.	
Battery Cabinet Dimension:	To be mentioned	
Battery Monitoring System (BMS):	UPS Shall have Battery Monitoring System that capable to monitor individual battery voltage, Battery Impedance (Ohmic Value), temperature, health etc. with graphical report.	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support	

RESTRICTED

	with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	
--	--	--

6. Isolation Transformer 200KVA

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Ortea/ Irem or equivalent))	
Model	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Rated power:	200kVA	
Input Voltage	3PH+N 400 Vac	
Output voltage:	3PH+N 400 Vac	
Type	Dyn11 – K20	
Windings	Copper	
Bypass	Inbuilt Maintenance By pass	
Fittings	Input and Output Circuit Breaker & Pilot Lamp	
Warranty	3 Years from the Date of Commissioning	

7. Floor Mounted Power Distribution System-100A with Auto transfer Switch for Server room

Feature List	Feature Description	Bidder Response
Model	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Maximum Total Current Draw per Phase	100A	
Nominal Input Voltage	400V 3PH	
Input Frequency	47 - 63 Hz	
Rack Height	To be mentioned	
Features	Multiple distribution options (3-phase and 1-phase)	

RESTRICTED

	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Local and web-based monitoring: Status available to customers both in the data center and remotely	
	Current Monitoring: Monitors the aggregate current draw per power distribution unit.	
	Network management capability: Full-featured network management interfaces that provide standards-based management via Web, SNMP, and Telnet.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
	Modular design: Provides fast serviceability and reduced maintenance requirements via self-diagnosing, field-replaceable modules.	
Auto Switch Features	Transfer (3-Phase) Minimum 2 incoming capable of 100A current per phase from bus-bar.	
	1 outgoing capable of 100A current per phase to Floor Mounted Power Distribution System.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 (Uptime Institute/epi) compliance in all aspects	
Warranty	Three (03) years full	

8. Floor Mounted Power Distribution System-50A with Auto transfer Switch for MMR-01&02

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	

RESTRICTED

Country of Manufacture	As per Tender Specification Article no 20	
Maximum Total Current Draw per Phase	50A	
Nominal Input Voltage	400V 3PH	
Input Frequency	47 - 63 Hz	
Rack Height	To be mentioned	
Features	Multiple distribution options (3-phase and 1-phase)	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Local and web-based monitoring: Status available to customers both in the data center and remotely	
	Current Monitoring: Monitors the aggregate current draw per power distribution unit.	
	Network management capability: Full-featured network management interfaces that provide standards-based management via Web, SNMP, and Telnet.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
	Modular design: Provides fast serviceability and reduced maintenance requirements via self-diagnosing, field-replaceable modules.	
Auto Switch Transfer Features (3-Phase)	Minimum 2 incoming capable of 50A current per phase from bus-bar.	
	1 outgoing capable of 50A current per phase to Floor Mounted Power Distribution System.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 (Uptime Institute/epi) compliance in all aspects	
Warranty	Three (03) years full	

9. IT Power Distribution Module 3x1 Pole 3 Wire 32A (1-Phase 32A Industrial Socket)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	230V	
Output Connections	(3) IEC 309 32A (2P+E)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

10. IT Power Distribution Module 3 Pole 5 Wire 32A		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 32A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

11. IT Power Distribution Module 3 Pole 5 Wire 63A		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	63A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 63A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

12. Rack Automatic Transfer Switch for single corded equipment		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/ Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Type	Automatic switching power redundancy to single corded equipment	
Form factor	Rack mountable horizontal 1U or 2U solutions	
Manageability	Network manageable through TCP/IP	
Transfer Time	Zero	
Capacity	At least 6 kW or higher	
LCD display for operating information	Should be inbuilt with the system.	
Ports	At least 6 ports or Higher	
Software Interface and	ATS Monitoring and Management Software and Ethernet interface from each ATS.	
	Provided software's functions should include monitoring and Controlling the ATS remotely through TCP/IP	
Firmware upgrades	On-the-fly firmware upgrades should be possible	
Event logging	Event logging with graphs should be possible in the proposed software	
Cables	12 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.	
	04 units of C20 to industrial female (32A)	
	02 units of C14 to industrial female (16A)	
	04 units of C19 to C20 cable (16A, 3m). 02 units of C19 to C20 cable (16A, 2m)	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

13. Transient Voltage Surge Suppression (TVSS)		
Feature List	Feature Description	Bidder Response
Brand	To be Mentioned (Preferably Schneider/ Rayvoss / Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Operating voltage, current and frequency	To be mentioned	
Features	Microprocessor-based controller	
	Plug-in modules for easy replacement	
Visual Indication	To be mentioned	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3/rated-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

14. Signal reference grid system		
Feature List	Feature Description	Bidder Response
General Feature	1. A separate & complete SRGS is to be designed and installed in accordance with applicable codes & standards for data center.	
	2. Separate SRG sub system for both MMR is to be design & combinedly will be connected with separate earthing system (N+N, 1 ohm each).	
	3. Separate SRG system is to be design for server room (All Server racks)	
	4. Seperrate SRG sub system for both Power room is to be design & combinely will be connected with separate earthing system(1 ohm).	
	5. Grid pattern of SRG will be followed the mesh system to secure floor pedestal	
	6. In SRG system proper copper strip, grounding clamp, UL listed bonding grids, low impedance raiser kit, BCF weld, BHO weld, Flat strip pedestal ground clamp, CPC pipe clamp are to be used.	

15. Data Center Earthing & Bonding system		
Feature List	Feature Description	Bidder Response
Bonding	1. Proper bonding for data equipment rack, telecommunication backbone, power cabinets, is to be designed & installed.	
	2. Proper & separate bonding network for power equipment, server rack, cooling system has to be interconnected with separate earth termination/ grounding system.	
	3. Bonding connection at all SRG mesh intersections & bonding between mesh & equipment is to be confirmed.	
SRG and Grounding	4. SRGs: The signal reference grid (SRG) system to be implemented for data center, MMR and power room separately.	
	5. Ground Resistance: The ground resistance has to be below 1 ohm.	
	6. General Requirement: All metallic object including cabinet, PDUs, Cooling system, raised floor etc. should be connected to grounding system.	
	7. For Rack/cabinet continuity	
	a. Racks should be assembled with paint piercing grounding washers, under the head of the bolt and between the nut and rack, to provide electrical continuity.	
	b. A full-length rack-grounding strip should be attached to the rear of the side rail with thread forming screws to ensure metal to metal contact.	
	8. For Rack/Cabinet Grounding: Larger bonding conductor to bond each rack or cabinet with the grounding strip to the data center grounding infrastructure (SRG System)	
	9. For Telecommunications Grounding Bar	
	a. Provision of larger conductor to bond the data center grounding infrastructure to the TGB.	
	b. Two hole copper compression lugs are preferred for vibration.	
	10. Telecommunications Bonding Bar	
a. The TBB should be installed as a continuous conductor, avoiding splices where possible.		
b. Avoid routing grounding/earthing conductors in metal conduits.		
11. Telecommunication Main Grounding Bus Bar		
	The TMGB is to be bonded to the service equipment (power) ground, which connects to earth ground (the grounding electrode system)	
	12. Supplier need to consider earthing meter installed to the separate earthing group for DC equipment (Present & Proposed data center)	
	13. Warranty: The vendor shall provide 3 years warranty.	

16. Data Centre Infrastructure Management system (DCIM)with energy & environment monitoring system with BMS		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/Vertiv/Sunbird/Commscope/Equivalent)	
Model name	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
No of device license required	At-least 1000 node license (If more no. of license is required to cover the full Data Center as per given requirement, have to be included)	
	If the proposed system is an appliance based, the appliance should be provided.	
Room Monitor	11	
Room Sensor	11	
Rack Monitor	50	
Temperature and Humidity Sensor with digital display	20	
Temperature and Humidity Sensor	20	
Spot Fluid Sensor	40	
Smoke Sensor	20	
Alarm beacon	20	
Vibration Sensor	20	
Door Switch Sensor for Rack	11	
Door Switch Sensor for Room	11	
Camera with sensor	45	
Tablet with pre-loaded Application	03 (at least 7 inch)	
Design Requirements:	All material and equipment used shall be standard components, regularly manufactured, available and not custom designed especially for this project. The data center infrastructure system, including the DCIM, shall previously be thoroughly tested as a system, and proven in actual use prior to installation on this project	
	The DCIM shall be installed on a physical server, or as a virtual appliance, with a specified HTTP or HTTPS connection to access the user interface (DCIM client), and standard TCP protocol connections for communications with the monitoring system	

RESTRICTED

	<p>The DCIM system-level redundancy and load-balancing shall be provided using a server-level cluster setup. Up to 4 servers should be setup in a cluster to gain performance improvements</p>	
	<p>The DCIM shall enable vendor-neutral inventory management with real-time device failures and data shown within a data center physical layout. Graphical floor layout and rack elevation view shall be supported from Day 1</p>	
	<p>The DCIM tool shall provide location-based drill-down views providing a structured overview of data center locations, from a global to local view down to single assets.</p>	
	<p>A Power Usage Effectiveness (PUE) dashboard will provide information on daily energy use</p>	
	<p>Inventory report provides structured information on all rack-mount devices, organized by device type, age, manufacturer, and properties for quick overview of all current devices within a particular data center</p>	
	<p>The DCIM tool shall have a search capability to allow data center operations to quickly locate a piece of equipment in the rack layout and floor layout.</p>	
	<p>The DCIM tool shall provide public web services API to allow third-party applications to access the inventory database, alarms and events, capacity and cooling analysis data, and PUE information</p>	
	<p>The DCIM shall provide provisions to predict the optimal location for physical infrastructure and rack-based IT equipment based on the availability and requirements of physical infrastructure capacity and user defined requirements such as redundancy, network, and business use grouping</p>	
	<p>The DCIM shall provide provisions to reduce stranded capacity and enable informed decision making and planning by proactively analyzing the impact of future moves, adds, changes before they occur, ensuring that the physical infrastructure provides the required space, power, and cooling capacity for current and future needs</p>	
	<p>The DCIM shall be capable of hosting additional add-on modules that allow a user to perform energy efficiency and energy cost management, inventory management, power and cooling capacity management, change management, IT optimization, IT power capping, server access (software Keyboard Video Mouse or KVM),</p>	

	dynamic cooling control and mobile data center management	
	The DCIM shall provide read-only smart phone applications to get a high level status of the data center operations and KPI	
	The DCIM shall be capable of integrating with additional plug-ins that supports Cisco UCS Manager, HP OneView, Vigilent dynamic cooling control, BMC Remedy ticketing system, Microsoft System Center Virtual Machine Manager 2008/2012, HP uCMDB, and VmwarevCenter, etc.	
DCIM Operation	<p>The DCIM software shall provide the methodology to create visual view of the data center floor layout, and the racks view and the equipment within, and manage network connectivity. This module shall also map the alarms to the appropriate device on the floor layout. The DCIM software shall support the following capabilities:</p> <ul style="list-style-type: none"> a. The DCIM tool will have the capability to add locations and rooms of different types to the data center model to represent the actual physical enterprise infrastructure. b. The DCIM tool will have the capability to configure a bird's eye view of the room layout to ensure the layout in the data center model accurately represents the real-world physical environment of the room. This includes any physical attributes of the room such as size, shape, doors, windows and walkways. c. The DCIM tool will have the capability to see multiple rooms in a layout pane at the same time allowing a user to compare or drag equipment between them – for modeling. d. The DCIM tool will have the capability to export the complete or filtered data center inventory into a delimited file (.csv file). e. The DCIM tool will have the capability to render the floor layout in both 2D and 3D view. f. Ability to import an AutoCad (.dwg) floor drawing and display the floor layout. Each 	

	<p>layer can be toggled on or off. Rooms can be created based on wall detection on the AutoCad drawing.</p> <p>g. Ability to export the Floor Layout to AutoCAD format (.dwg). Each overlay and the information in the overlay must be stored in individual layers.</p> <p>h. Ability to export the Floor Layout to the following picture formats: BMP, JPG, PNG and SVG.</p> <p>i. Ability to export the Rack View to the following picture formats: BMP, JPG, PNG and SVG.</p> <p>j. Ability to copy/paste equipment on the floor, such as racks, PDUs, UPS and cooling units as well as equipment in the racks, such as servers and patch panels.</p>	
<p>Multi-tenant Data Center Support</p>	<p>a. Ability to create cages and auto-detect cage area in square meters or square footage.</p> <p>B. Ability to create cages automatically from AutoCAD drawing through cage selection and wall detection.</p> <p>C. Ability to assign customer to data center asset including rack mounted equipments, racks, cages, etc.</p> <p>D. Cages, racks and servers are color coded based on sales status (closed, reserved, internal, and open).</p> <p>E. Ability to assign Contracted Power value to each cage, rack or server.</p> <p>F. Ability to add power receptacles to each cage.</p> <p>G. Show a legend on the floor view with information about how many racks are open, closed, reserved and internal.</p> <p>H. Show a legend on the floor view with information about how much space is open, closed, reserved and internal.</p> <p>I. Show a legend on the floor view with information about total room area, sellable space and space efficiency.</p>	
<p>Rack elevation View</p>	<p>A. The DCIM tool will identify how much weight has been placed in a rack / room compared to the predefined load bearing capability settings of the rack.</p>	

RESTRICTED

	B. Illustrate the weight of the equipment added to the rack in the rack layout compared to the maximum equipment loading capability of the rack.	
	C. Visualize status of network ports on equipment (used vs. not used).	
	D. Visualize network cables.	
Network Management	A. The DCIM tool will be able to model the configured network connections and allows a user to setup new network routes between the configured equipment.	
	B. Network port properties will have the capability to be imported from a product catalog and/or will be user configurable.	
	C. Ability to configure network routes for selected network equipment in the layout, for example between a server and a switch or a switch and a switch. A route is defined as a connection from a piece of equipment (communication endpoint, such as a server or layer 2/3 network gear, such as a switch) to the first piece of equipment that is a communication endpoint or layer 2/3 network gear.	
	D. Ability to configure cable types and color code each cable type.	
Product Catalog	A. The DCIM tool will be able to provide a product catalog that contains up-to-date floor and rack mounted data center equipment.	
	B. The DCIM tool will be able to allow a user to add floor and rack-mountable equipment to a rack, server room, electrical room or store room.	
	C. Ability to create an inventory bundle that combines multiple pieces of equipment in one building block.	
Dashboard Key Performance Indicator (KPI) View	A. Provide a map view to monitor the data center operations in a quick overview, including any alarms in different locations and rooms.	
	B. From the map overview, one can drill down to locations > rooms > racks > servers for details or troubleshooting.	
	C. Display capacity KPIs for each data center in the map view. The KPIs should include the status of the Power, Cooling, U-space and Network utilization.	
	D. Power is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	
	E. Cooling is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	
	F. U-space is represented as the percentage	

RESTRICTED

	of the available U-positions (U-pos) that is populated with equipment in the location or room.	
	Network is represented as the percentage of the available Network ports (ports) that is utilized by networking equipment in the location or room	
Data Center Operation: Capacity	The DCIM software shall provide capabilities to perform capacity planning, create capacity groups, perform power and cooling analysis as per the following details:	
Capacity Planning	The DCIM software will provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, network and power capacity to optimize capacity utilization and avoid stranded capacity:	
	A. Impact simulation: Generates a list of equipment that would be impacted if the selected piece of equipment, e.g. a UPS or cooling unit, was to fail.	
	B. Measured Load: Display measured load data for UPS and racks in the floor layout that identify how much of each UPS or rack's maximum kW power is in use. This requires communication to power monitoring devices or servers.	
	C. Measured Load: Displayed measured load data for cages in the floor layout that identify how much of a cage's contracted power is in use. This requires communication to power monitoring devices or servers.	
	D. Power Capacity: Ability to assign planned capacity for each rack and illustrates rack capacity consumption compared to the planned recommended values for that rack. Provide information such as remaining power, the amount exceeding the recommended capacity.	
	E. Power Path: Ability to model power connections between the equipment supplying and delivering power and the equipment requiring power. This includes power path from switchgear, UPS, main PDU with modular circuit breaker mapping, rack RPDU and to individual servers.	
	F. Power Path: Ability to export the power path to a comma separated file.	
	G. Rack U Space: Ability to monitor and display rack U space utilization of each rack.	
Capacity Groups	Ability to model capacity groups that allows a user to group equipment's, placing it in groups of racks with similar power capacity requirements to match the IT equipment with availability needs and avoid	

RESTRICTED

	stranded space, power, and cooling capacity. For example, group a set of high-density racks together for optimized power and cooling configuration.	
Power Analysis	Ability to detect the following list of configuration issues regarding data center power configuration and provide recommended actions:	
	A. Connection has not been configured between PDU and power supply: A power connection is missing in the data center model from this PDU to the power supply from which it should receive power.	
	B. Equipment connected to this PDU draws more power than is supported by the power supply breaker: The breaker does not provide sufficient power to cover the power requirements of the equipment connected to that PDU.	
	C. Equipment is connected to a rack PDU outside this rack: The power connection setup for this equipment is not optimum as it is setup to be supplied by a rack PDU that is not positioned in the same rack as the equipment.	
	D. Internal redundancy setup for UPS and group must match: The internal redundancy setup for the UPS and group does not match, for example N and N+1.	
	E. Rack is without rack PDU or a rack PDU is not powered: The rack is without rack PDUs or its rack PDUs are not connected to a PDU, remote distribution panel (RDP) or power panel.	
	F. The breaker configuration does not support rack's estimated load: The equipment in the rack draws more power than the breaker supports. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.	
	G. The input voltage setting required by the equipment is not available in current rack: In the data center model, the server's input voltage requirement cannot be supplied by the rack PDU in the rack.	
	H. The measured load exceeds the estimated load per phase designed for the rack: Connected devices in the rack use more power than the estimated load per phase in the rack shall be indicated in the data center model.	
	I. The measured load exceeds the total estimated load configured for the rack: Connected devices in the rack that use more power than the total estimated load in the rack shall be indicated in the data center model.	

RESTRICTED

	<p>J. The measured load of the UPS exceeds the total estimated load of the connected equipment: Devices connected to the UPS use more power than design capacity or they have not been assigned to the correct UPS in the data center model layout to correctly represent the physical infrastructure. In case of 3 phase equipment, the problem shall be indicated even if the measured value is only too high for one of the phases.</p>	
	<p>K. The phase configuration for the connected server is not supported by the rack PDU: The phase connection configured for this server is not valid. This message will occur if a power connection had been configured to this server but subsequently changes have been made to the phase configuration.</p>	
	<p>L. The Rack PDU output voltage setting does not match the output voltage of the connected PDU / Power Panel: The power connection is invalid because the voltage required by the rack PDU is not available from the power distribution component.</p>	
	<p>M. The server must be supplied from the same phase from both distribution units: The redundancy setup requires identical phase distribution setup for A and B feed.</p>	
	<p>N. The UPS in the layout does not supply enough power to match the configured load of connected equipment in the layout: The load of the equipment connected to the UPS is higher than the load that the UPS can supply. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.</p>	
Cooling Analysis	<p>A. The DCIM software shall be able to calculate cooling performance of data centers in real-time with CFD-like simulation, provide calculated inlet and exhaust temperatures per rack plus capture index (percentage of heat captured by cooling devices) per rack.</p>	
	<p>B. Ability to present the calculation results visually in the floor layout.</p>	
	<p>C. Ability to alarm cooling configuration issues and provide recommended actions. For example, a room has no perforated tiles for the Computer Room Air Conditioning (CRAC) unit airflow (one or more CRACs have been added to the floor but no perforated tiles have been added), or there is no perforated tile airflow (one or more perforated tiles have been added to the</p>	

	room but no CRACs have been provided to supply any airflow).	
	D. 2D plenum airflow and pressure view: Provide a 2D under-floor plenum view that shows airflow vectors and Cubic Feet per Minute (CFM) based on the height of the raised floor, the placement and type of perforated tiles and cooling devices. When a cooling unit or a perforated tile is moved around, the flow vectors and airflow CFMs shall update instantly.	
	E. 3D temperature and airflow view: Provide a 3D view showing max/average inlet/return temperature and airflow above the raised floor. Calculate velocity vector and temperature in real-time (seconds) to allow customers to try what-if scenarios. Ability to slide the temperature and velocity plane in all three dimensions.	
	F. Ability to simulate failure of one or more cooling units and examine impacts to IT equipment.	
	G. Ability to map temperature sensors to rack elevation or anywhere in the data center 3D space and draw the 3D measured temperature map based on the measured data.	
Integration with 3rd Party Software	A. The DCIM software shall support integration with Cisco UCS manager to retrieve real-time power measurement data for blade servers and display them. In addition, it should support automatic power capping Cisco UCS chassis based on rack PDU breaker setting to safe guard rack PDU breakers.	
	B. The DCIM software shall support integration with VmwarevCenter and Microsoft System Center Operations Manager (SCOM), Virtual Machine manager to retrieve virtual machine information and map them to physical servers.	
	C. The DCIM software shall support integration with HP Universal Configuration Management Database (uCMDB), pushing IT asset data such as network, server devices and properties to the DCIM software.	
	D. Ability to support two-way data exchange between the DCIM software and a broad range of systems, such as CMDBs, asset management systems, and building management systems using Extract, transform and load (ETL). Based on the ETL system, it is possible to develop custom solutions, integrating DCIM with a broad range of data	

	sources.	
Data Center Operation: Energy Efficiency	The DCIM shall provide the following functionality from the data center Energy Efficiency point of view	
	1. The DCIM tool will provide current and historical Power Usage Effectiveness (PUE) values and full insight into current and historical energy efficiency.	
	2. It will present how much power is devoted to driving the installed IT-equipment compared with the total facility consumption.	
	3. Identify efficiency losses and enables improved PUE at the subsystem level.	
	4. Provide insight into energy losses and cost of energy at the subsystem level, providing details of which subsystem draws the most costs.	
	5. The DCIM tool will have a web-based dashboard view which includes efficiency data on current and historical PUE, as well as detailed subsystem cost analysis.	
	6. The DCIM tool will provide a report on current and historical PUE values.	
7. The DCIM tool will provide energy efficiency analysis, PUE and DciE (Data Center infrastructure Efficiency) reporting.		
Data Center Operation: Change	The DCIM shall provide the following change management functionality to keep track of additions, movements, maintenance or deletions in a data center:	

17. Controlled electric lighting system (Electric lighting & Emergency Lighting) (Quantity: 1 Set)		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Features		
Data Center Lighting & cabling	The data center automatic & manual lighting system with required cabling is to be design & installed by bidder. Lighting & interior design must be vatted from BNNET acceptance committee.	
Emergency Lighting Control	When the normal AC power fails, the emergency lighting system should sense the power failure and immediately switches to the emergency mode, illuminating more than 5 lamps at a time.	
	When AC power is restored, the emergency lighting	

RESTRICTED

	system should returns to the charging mode until the next power failure	
No of Emergency Light	To be mentioned	
Central Control Panel	The central control panel should include all the power lighting and also the emergency lighting for allowing monitoring and control of Data center lighting system.	
Total Floor Area	As per drawing	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

18. Electrical Works		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Electrical DB Panels & DB Accessories		
	Supply & installation of Electrical Panels housed in 2.0mm standard sheet steel enclosure type tested, fixed Type, compartmentalized, totally enclosed, free standing, Floor mounted type, dust and vermin Proof, duly wired up and ready for installation at site. All MCB, MCCB & ACB should be Ics 100% Icu. The boards are designed and constructed in accordance with IEC61439-6. Busbars and other live parts are spaced and insulated in accordance with IEC standard. All DB should C911:C925	
	The DB system should have following features: a. Factory assembled power distribution module with breaker position monitoring. b. No rear access c. Network management via web interface, SNMP, modbus and other appropriate interfaces. d. Compatible with Tier -3 data center. e. Self diagnosing module and tool less module replacement f. Output metering and branch circuit/current monitoring. h. Local access display interface	
	Technical Description	
AVR Output DB-	Bidder will design & proposed required DB for AVR,	

RESTRICTED

01	Online UPS, HVAC, FMPDU, others utility load as per attached to comply with tire-3 Standard. During design bidder will consider appropriate bus bar, breaker, protection devices, monitoring devices for SCADA/DCIM monitoring.	
AVR Output DB-02		
MDB-01		
MDB-02		
HVAC DB-01		
HVAC DB-02		
SECURITY DB-01		
SECURITY DB-02		
UPS O/P DB-01		
UPS O/P DB-02		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

19. Power Cabling and Others related works		
Brand	To be mentioned (Preferably BRB or equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Cable Requirements	Bidder's has to quote cabling for complete Data Center.	
	All connection of UPS, AVR, RACK and other electric items (approx. 24 Nos. Rack) inside the data center through IT Power Distribution Modules.	
SLD Diagram	Bidder has to provide Complete SLD starting from Sub-station to IT load	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

20. Power Cable Ladder		
Feature List	Feature Description	Bidder Response
Brand	To be mention	

RESTRICTED

Model	To be mention	
Origin	As per Tender Specification Article no 20	
Country of Manufacturing	As per Tender Specification Article no 20	
Type	Metal Steel/Stainless Steel Mesh Type Electrical ladder	
Cable ladder size	width 12"	
Height	Approx. 2"/Customized	
Materials	U Steel cable ladder with electro zinc plated treatment. Thickness: Min.1.6 mm and average load of more than 200KG per meter.	
Color	Powder coating White or Silver or Siemens Gray	
Installation material	Thread Rod/Hanger (max 3'), Flat BAR, Clump, Royal Bolt, Screw, Saddle, bending/L-shape, T-Shape etc. for hanging/vertical /Horizontal area both the overhead and under raised floor	
Power Cable Tray	Cable Tray	

21. Electrical Switch Sockets

Feature List	Feature Description	Bidder Response
Electrical Switch Sockets	Brand: To be mentioned	
	Country of Origin: To be mentioned	
Industrial Socket 32A SP		
	Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge	
	Supply and installation of imported gang switches& socket and wall boxes complete with all other necessary accessories and connections everything complete as per	

RESTRICTED

	drawing, specification and instruction of the Engineer-in-charge. The wall boxes may be locally made of 18SWG galvanized steel sheet including earthing block. (Maximum Current 13 Amps)	
	3-Pin wit 2 pin socket	
Switch for Light	Supply and installation of imported 13A, 220V, combined switched socket outlet including the box, cover plate with necessary galvanized machine screws, earthing block complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge. The box may be locally made of 18SWG galvanized sheet steel. Maximum Current 10 Amps	
	3 Gang Switch	
	4 Gang Switch	
	2 Gang Switch	
Lighting System	Supply of ceiling surface/concealed mounted light fixture complete with energy saving LED light, best quality lighting shade with mounting kit and all other necessary materials as per drawing, specifications and direction of the Engineer-in-charge.	
	Recessed Ceiling Luminaires, Series for LED panel light 2'x 2' with hanging accessories	
Emergency light with battery back up		
Brand:	Any international Reputed Brand	
Model:	To be mentioned by bidder	
General Features	Emergency light luminaire	
	Input: 220VAC +/- 10% 50 Hz 1 phase	
	Bulbs: 2 x 9W & 12 W SMD LED super wide beam 90 Deg.	
	Lamp: Aluminum heat sink body and plastic diffuser 180 Deg. Adjustable legs	
	Automatic solid-state system	

RESTRICTED

	Constant current charger	
	10-12 Hours charging duration	
	Battery Nickel Metal hydride (Ni-MH)	
	Battery protection: Low voltage cut off	
	System protection: high voltage cut off	
	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: front cover 1.5mm electro-galvanized steel sheet with epoxy powder coated and stove enamel	
	Operation temperature: 10 Deg. - 40 Deg.	
	IP rating: IP 20	
	Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)	
	TIS.1102-2538 (self-contained emergency light Luminaries)	
Emergency Exit Sign	Wall and ceiling mounted	
Brand	Any international Reputed Brand	
Model	To be mentioned by bidder	
General Features	Input: 220VAC +/- 10% 50 Hz 1 phase	
	Lamp: SMD Surface mount	
	Autometic solid state system charger	
	Constant current charger	
	10-12 Hours charging duration	
	System protection: high voltage cut off	
	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: Electro-galvanized steel sheet 1mm & front plate 1.5mm epoxy powder and stove enamel coated anti-rust corrosion proof	
	ISO green legend	
	Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)	

RESTRICTED

	TIS.1102-2538 (self-contained emergency light Luminaries)	
Electrical Accessories	Accessories: Lugs, Heat Shrink, Cable tie, Screw, GI wire, Royal Plug, Royal Bolt, Clump, PVC Tape, Masking Tape, Rivet, High Quality nylon Fastener etc.	

22. Precision Air Conditioner (PAC)_DX for Server Room		
Products Names/Items	Description of requirements	Bidder Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 60 kW	
Total sensible capacity	Minimum 60 kW	
Net Total Capacity	To be mentioned	
Net Sensible Capacity	To be mentioned	
Air Flow (Indoor)	To be mentioned	
Air Flow(outdoor)	To be mentioned	
Ambient Temperature	45 °C	
Fan Technology	EC Fan Technology	
Electrical power consumption	To be mentioned	
Energy Efficient Ratio (EER)	To be mentioned	
AER	To be mentioned	
Total power consumption	To be mentioned	
LpA (2m free field)	Indoor: 65.4 dB(A)	
LpA (5m free field):	Outdoor: 57.9 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative	50%	

RESTRICTED

humidity		
Altitude above sea level:	100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 3 (three)	
Heat rejection	To be mentioned	
Condenser capacity	To be mentioned	
Compressor type	Scroll Type	
Expansion Valve	Electronic	
Electrical Heating	To be mentioned	
Steam humidification	To be mentioned	
Refrigerant	R407C	
Number of refrigerant circuits	Minimum 2 (two)	
Compressor:	Minimum 2 (two)	
Filter	To be mentioned	
Controller	a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
	b) Controller based Sequencing Facility c) water leak detector	
	c) Auto Shutdown by external fire alarm	
	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	
Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen, Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper	

RESTRICTED

	evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

23. Precision Air Conditioner (PAC)_DX for MMR & Power Room		
Description	Required Specification	
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin :	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 14.8 kW	
Total sensible capacity	Minimum 12.9 kW	
Net Total Capacity	Minimum 14.1 kW	
Net Sensible Capacity	Minimum 12.2 kW	
Air Flow (Indoor)	Minimum 3,600 m ³ /h	
Air Flow(outdoor)	Minimum 10,600 m ³ /h	
Ambient Temperature	42 °C	
Fan Technology	EC Fan Technology	
Electrical power consumption	Maximum 3.6 kW/Compressor.	
Energy Efficient Ratio (EER)	3.44 kw /better	
Total power consumption	Maximum 4.3 kW	
LpA (2m free field)	Indoor: 56.2 dB(A)	
LpA (5m free field):	Outdoor: 51.1 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air	14-16 degree Celsius	

RESTRICTED

temperature		
Return air relative humidity	50%	
Altitude above sea level:	100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 1 (one)	
Heat rejection	18.6 kw (per compressor)	
Condenser capacity	18.6 kw each condenser	
Compressor type	Scroll Type	
Expansion Valve	Electronic	
Electrical Heating	9 to 18 kw or more	
Steam humidification	8 to 15 kg	
Refrigerant	R407C	
Number of refrigerant circuits	Minimum 1 (one)	
Compressor:	Minimum 1 (one)	
Filter	To be mentioned	
Controller	a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
	b) Controller based Sequencing Facility c) water leak detector	
	c) Auto Shutdown by external fire alarm	
	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	
Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen, Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in	

RESTRICTED

	proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

24. Chiller		
Chiller	<p>The Chiller is an air-cooled, high-efficiency range designed for industrial cooling, IT, and comfort applications that require intensive, year-round use (24/7/365).</p> <p>The entire range is equipped with micro-channel condensers, shell-and-tube evaporators, semi-hermetic screw compressors with capacity slides, low GWP R513A refrigerant, electronic expansion valves, and axial fans with phase-cut modulation or EC brushless technology. It also includes SEC.blue electronic control. All chillers are available in Free Cooling and/or Low Noise versions.</p>	
Brand:	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	As per Tender Specification Article no 20	
Country of Shipment:	To be mentioned	
Bearing structure	The chiller is manufactured with a bearing structure made of painted galvanized steel profiles assembled with A2 stainless steel small ironmongery. To ensure proper solidity and corrosion resistance, all metal components are made of structural steel complying with UNI EN 10346, with DX51D-type steel and Z200-type coating.	
Electrical cabinet	<p>Electrical cabinet installed on the short side of the chiller, with components and construction in accordance with European regulations CEI EN 60204-1, CEI EN 61000-6-2/4 and EMC 2014/30/UE.</p> <p>Triple leaf metal frame with lock and "double-bit 3-5" key, IP44 degree of protection for outdoor installation</p>	
Refrigerant	The chiller use R513A not flammable refrigerant gas ensuring low environmental impact, no ozone damage (ODP = 0) and a reduced Global Warming Potential (GWP = 573).	

RESTRICTED

General		
Cooling capacity:	Minimum 130 KW by 2Unit	
EER:	To be mentioned	
Total absorbed Electrical power:	To be mentioned	
S.E.P.R.	To be mentioned	
Ambient temperature working limits	min -10 max 48 °C	
Application	Outdoor	
Outlet water temperature working limits	min 0 max 15 °C	
Refrigerant:	R513A	
Main power supply:	400V/3/50 (V/Ph/Hz)	
Secondaries voltage	230 Vac	
Absorbed electrical power (FLI)	To be mentioned	
Absorbed current (FLA)	To be mentioned	
Inrush current (MIC)	To be mentioned	
COMPRESSORS		
Compressor type	Screw	
Number of Compressor	Minimum 1(one)	
Number of refrigerant circuits	Minimum 1(one)	
Absorbed Electrical power	To be mentioned	
Absorbed electrical power (FLI)	To be mentioned	
Absorbed current (FLA)	To be mentioned	
FANS		
Fan	3 x ø910	
Fans type	EC	
Air temperature	35 °C	
Fans part load	100%	
Fan air flow	To be mentioned	
Absorbed power at working point	To be mentioned	
Max absorbed electrical power	0 KW	

RESTRICTED

(FLI)		
Absorbed current (FLA)	To be mentioned	
HYDRAULIC		
Chilled fluid	Water	
Fluid freezing temperature	0 °C	
Max working pressure	PN 10	
Chilled fluid inlet temp.	12 °C	
Chilled fluid outlet temp.	7 °C	
Fluid flow rate	To be mentioned	
Pressure drop	To be mentioned	
Head pressure available	To be mentioned	
Chilled fluid flow rate	To be mentioned	
Chilled fluid flow rate	To be mentioned	
Width x Height x Depth	To be mentioned	
Weight empty	0 Kg	
Hydraulic connections	3 " M Vic	
Sound pressure level	Maximum 57.5 dB(A)	
Sound power level	Maximum 89.5 dB(A)	
The chillers designed and manufactured in compliance with the EC directive and the EN safety regulations listed below:		
	UNI EN ISO 9001: Quality Management System;	
	UNI EN ISO 14001: Environmental Management;	
	2006/42/EC: Machinery Directive;	
	2014/30/UE: EMC Directive;	
	2014/68/UE: Pressure Equipment Directive;	
	EN 378-1, 2: Refrigerating systems and heat pumps;	
	EN ISO 12100 -1: Safety of machinery;	
	EN ISO 13857: Safety of machinery - Safety distances;	
	EN 60204 -1: Safety of machinery - Electrical equipment;	
	EN 61000-6-2: Immunity for industrial environments;	
	EN 61000-6-4: Emission standard for industrial environments;	
	2009/125/EC: Directive EcoDesign.	
Outdoor installation	All electrical components subject to atmospheric agents have minimum protection degree of IP44	

25. Chilled Water (CW) Air Handling Unit for Server Room		
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Water cooled	
Unit configuration Type	Down Flow.	
Total Cooling capacity	Minimum 60 kW	
Sensible Cooling capacity	Minimum 60 kW	
Net total cooling capacity:	To be mentioned	
Net sensible cooling capacity:	To be mentioned	
Air Flow (Indoor)	To be mentioned	
Fan Technology	EC Fan Technology	
Total power consumption:	To be mentioned	
Energy Efficient Ratio (EER)	To be mentioned	
AER	To be mentioned	
LpA (2m free field)	61.5 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50 rel.%	
Altitude above sea level:	Minimum 100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 2 (two)	
ESP external static pressure:	20 Pa	
Total pressure drop:	To be mentioned	
Filter	To be mentioned	
2 way-control valve for chilled water control	a) 2-way control ball valve for capacity control of the heat exchanger respectively to control the unit capacity	
	b) continuously variable by 0-10V control signal from the controller of the A/C unit	
	c) valve can be manually operated in case of emergency.	

RESTRICTED

	d) one control valve per circuit	
	e) valve size, valve type, internal valve structure optimized on stable control properties in full load and part load operation	
Dimension (H x W x D):	To be mentioned	
Weight:	To be mentioned	
Voltage	400V/50Hz/3Ph/N/PE	
Electric cabinet/Electrics :		
	Electric cabinet (electric box) integrated in the A/C unit for accommodation of all high voltage and control components; design according to EN 60204-1; protection class: IP20	
	Located in upper front area of the unit; accessible for maintenance exclusively from the front	
	Clear and space saving structure of all high voltage and control components	
	Consistent separation of high voltage and control elements to avoid EMC interferences. This improves the resistance against electro-magnetic noise.	
	All three-phase consumers protected against overload and short circuit by circuit breakers according to IEC/EN 60947-1	
	Completed wiring of motor circuit breakers, contactors and control components in wiring ducts	
	Top hat rail or busbar system for high voltage components	
	Installed main switch (3 poles) operable from the outside, design as load disconnecter	
Installation and Commissioning	Installation and Commissioning should be done by OEM certified Engineer.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

26. VESDA System(Very Early Warning Aspirating Smoke Detection) for DRDC Server & Power Room with Uptime compliance Zone separation		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Honeywell / Eaton / Xtralis / Bosch / Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Capacity	The proposed solution should be for 4,000 sft. Floor space.	
	The total electric load will be calculated for 24 Racks where each Rack will consist of 5KW load (avg.)	
Additional equipment	Control panels.	
	Releasing devices	
	Remote manual pull stations	
	Corner pulleys	
	Door closures	
	Pressure trips	
	Bells and alarms	
	Pneumatic switches	
	Good to have TCP/IP base remote control capability from Day 1.	
Fire Detection System	Automatic detection for early warning of fire.	
	Should be able to identify different types of smoke.	
	Smoke detectors for gas discharge.	
	The detection circuits should be configured using coincidence or independent inputs.	
Other	If any other components have to be added to design and install the solution To be mentioned and quote the same.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

27. Automated Fire Suppression System for DRDC Server, MMR, Battery & Power Room		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Name of the GAS agent	NOVEC-1230	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
General Features	<p>a. The automatic fire suppression system design shall be strictly as per NFPA standard.</p> <p>b. It should be a Clean Agent Gas Based Automatic Fire Suppression System.</p> <p>c. The Seamless storage cylinder shall be for fire suppression system.</p> <p>d. The Valve operating actuators shall be of Electric (Solenoid) type. The actuators should be capable of being functionally tested for periodic servicing requirements.</p> <p>e. The individual cylinder bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure. This mechanism should be integrated as part of the actuator.</p> <p>f. The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.</p> <p>g. The detection and control system that shall be used to trigger the suppression shall employ cross zoning of smoke detectors. A single detector in one zone activated, shall cause an alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.</p> <p>h. The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc.</p> <p>i. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final</p>	

RESTRICTED

	<p>number of the discharge nozzles shall be according to the OEM's patented and certified software.</p> <p>j.Manual Gas Discharge stations</p> <p>k.Manual Abort Stations shall be provided</p> <p>l.Manual Gas Discharge stations</p>	
Gas Suppression Solution	Bidder will propose solution as per drawing & requirement.	
Refill	The system should be easily refillable	
Refill Support	The proposed Gas should be refillable up to year 2035.	
	Proper document should be provided to support the time line 2035.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

28. Portable fire extinguisher ABC Dry Powder		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Material	ABC Dry Powder	
Weight	10Kg each	
Wall hanging kit	To be provided from day one.	
Powder life time	Should be 2years or above.	
Accessories	If any accessories required necessary should be provided.	
BOM	BOM to be attached with technical compliance of each item	

RESTRICTED

Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

29. Portable fire extinguisher CO₂

Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Material	CO ₂	
Weight	5Litter each	
Wall hanging kit	To be provided from day one.	
Powder life time	Should be 2years or above.	
Accessories	If any accessories required necessary should be provided.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

30. Access Control with visitor management System (Quantity: Combination of IRIS (1unit), RFID & Biometric (14 unit) including 15 unit Exit Reader,)]

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell or Equivalent)	
Model No.	To be mentioned	
Country of	As per Tender Specification Article no 20 and South	

RESTRICTED

Origin	Korea	
Country of Manufacture	As per Tender Specification Article no 20	
	All the active components quoted for Access control system must be from a single OEM	
ACCESS CONTROLLER & Components	ACCESS DOORCONTROLLER UP TO 4 WIEGAND reader support	
	The access controller must be a rail mountable device for use in specific enclosures as well as existing standard 19" racks	
	The controller shall have a modular design with downloadable software so that the application program can be easily updated without touching the controller itself	
	Latest integrated 32-bit, 30 Mhz Micro-controller based system architecture;	
	On board Real Time Clock that will adjust itself to leap year computations automatically	
	ACCESS DOORCONTROLLER shall have 8 Relay outputs; 8 Analog Inputs; onboard LCD display 16 Characters	
	16-characters liquid crystal display (LCD), shall display network parameters and actual status like:	
	a. IP address of the controller	
	b. MAC address of the controller	
	c. DHCP on/off	
	d. Status of all the inputs connected to it	
	e. Status of all the outputs connected to it	
	f. Online and Offline status of the controller	
	g. Firmware version	
	ACCESS DOORCONTROLLER shall include a standard 2GB Compact flash (CF) memory card for storing cardholder data and access events.	
	Memory shall store database that has a capacity with a minimum of 80,000 cardholders and Event buffer size: maximum of 4,00,000 events with date and time stamp.	

RESTRICTED

	The access controller is UL 294, CE approved.	
	ACCESS DOORCONTROLLER housing shall be in accordance with UL 294 approved and is used for securely mounting and housing the Access Controller, extensions and the power supplies	
	Power supply with battery charger for ACCESS DOORCONTROLLER Shall be with Selectable 12 VDC or 24 VDC voltage output Overvoltage protection Regulates battery charging voltage The product is classified in accordance with the following standards: <ul style="list-style-type: none"> • EN 55022 Class B • EN 55024 • IEC / UL / EN 60950 & CSA (product safety) • CE The Power supply can be mounted on rails and installed in the housing	
Biometric Smart Card Reader	The Finger-print biometric reader provided shall be of ruggedized design, having weatherized polycarbonate enclosure or similar protection to withstand harsh environments for both indoor/outdoor used and provides a high degree of vandal resistance with surface mounting style 13.56 MHz Biometric smart card Reader readers as per tender specifications	
	Biometric readers shall have CPU: ARM® CortexTM-A9 core 1GHz Biometric reader shall be with FBI PIV IQS certified optical fingerprint sensor Operating conditions: Temperature: -20°C to 55°C (-4°F to 131°F) – Humidity: 10% to 80% (non condensing) Ingress protection: IP65 Shall have 500 user capacity with expansion capacity of upto 10,000 users Accuracy shall be maintained regardless of number of users in database Biometric reader shall be with 2.8" QVGA color touchscreen and buzzer The specifier shall supply and install the necessary software to manage the Finger-print enrollment for all users and configuration of the Finger-print access control operations. The software provided shall be integrated to the Access Control System for access	

	control and monitoring.	
Smart Reader	<p>Card</p> <p>The Contact less Smart card reader shall provide authentication by reading the Card ID & controller will compare with database and actuating the barrier/turnstile.</p> <p>Contactless smart card readers shall comply with ISO 15693 and shall read credentials that comply with these standards</p> <p>It shall be plug & Play type with suitable locking devices.</p> <p>It shall operate on its own. No software control is required for configuring the threshold sensitivity for readers</p> <p>It shall be possible to exchange the smart card reader without needing to reprogram the control unit</p> <p>The fault of /at one smart card reader shall not affect the functioning of other smart card readers on the network.</p> <p>The readers shall be powered by field panels itself.</p> <p>No external power supply should be used for powering the reader</p> <p>The Card reader shall confirm to ISO 14443</p> <p>The Card reader shall be capable of reading the selected card technologies. (HID iClass/MiFareDESFire EV1 within the 14.56 MHz range).</p> <p>Shall use 64-bit authentication keys to reduce the risk of compromised data or duplicate cards. The contactless smart card reader and cards shall require matching keys in order to function together. All RF data transmission between the card and the reader shall be encrypted, using a secure algorithm.</p> <p>It shall have a read range of 5 cm – 7.5 cm when used with the accepted compatible access card technology</p> <p>It shall be capable of providing a unique tone and/or tone sequences for various status conditions such as access granted, access denied, reader power up, etc., and clear visual status LED indication (multi color) shall be provided for various status conditions.</p>	
	<p>Enhanced & optimized multi-tag inventory algorithm with the reading speed of more than 100 tags per second.</p> <p>Built-in 9dBi circular polarized antenna to read an RFID tag in any orientation from vehicle's windshield</p> <p>Supports INDIA 865~867 MHz, EU 865~868MHz, US 902~928MHz working frequency</p> <p>Reliable read distance of up to 12 meters with</p>	

RESTRICTED

	<p>IDCUBE's specialized ASSA series of long-range credentials Support EPC Global UHF class 1 gen2 / ISO18000-6C protocol RFID tags Integrates with Wiegand/RS232 compatible controllers Support for command, polling and trigger mode</p>	
Smart Cards	iCLASS Seos Contactless Smart Card, 8K memory	
	<p>AES-128/2TDEA cryptographic algorithms for data protection Mutual authentication protocol with generation of diversified session key to protect each card session (using secure messaging)</p>	
	Supports ISO/IEC standards: 7810, 7816 and contactless cards (14443 A)	
	<p>Operating Temperature: - -40 to 70 degrees C and Operating Humidity 5% to 95% relative humidity non-condensing</p>	
Access Control Software	<p>The Access Control System shall have a multi-level priority interrupt structure proven in multi-tasking and multi-client real time applications. Simultaneous alarms/events monitoring by multiple users, system supervision and history archiving shall be possible without degradation of any functionality specified for system or operation.</p>	
	The Access Control System server shall act as the source that provides time synchronization across all sub-systems.	
	<p>The Access Control System shall be capable to support to the following with additional expansion licenses if required:</p> <ul style="list-style-type: none"> • Number of active cardholders – 400,000 • Number of readers – 10,000 • Number of access groups – 255 • Number of time schedules – 255 • 4 – 8 digits programmable (Personal Identification Number) PIN codes • Remote Online Locks – 1,000 • Map viewer floor plans – 1,000 	
	<p>Operating Environment: The system server shall be use latest edition of Windows Server 2016 / 2019 and Client shall support Windows 10 shall include network capability with the TCP/IP data communications network protocol and hardware</p>	

	<p>Graphical User Interface: The system shall be a flexible and user-friendly workstation providing user(s) with a Graphical User Interfaces (GUIs) for alarm monitoring and control that includes map viewer with alarm list and a swipe ticker for visual door monitoring. The Access Control System GUI shall support single or multi screen displays having multiple dialogs separately. In case of alarms, the map will automatically focus on the alarm location.</p>	
	<p>Map Viewer and device overview: The system shall contain a map viewer. This map viewer shall provide a graphical presentation of the premises by means of floor plans, pictures or any desired graphical representation. On the maps entrances and devices like MAC, AMC, readers and digital input/outputs can be positioned as a dynamic icons. These graphical icons will display the location of the device in the map and the actual status of the device. Every icon can be displayed in several sizes, angle and color and background color. Clicking any of the devices automatically shows the commands available for controlling the respective device. Control commands are automatically linked based on device type. An operator can be assigned one or multiple authorizations for parts of the map viewer, such as door commands, reader commands, controller commands, system commands, special door commands, digital output commands, alarm list commands, swipe ticker commands. An area overview shall be able to show name, type (e.g. parking), current count, maximum count and state (e.g. empty, full). The ACS System must provide a real-time device overview of the entire system's status. All connected devices are shown on a status tree. A direct control into subsystems is possible by clicking on panel/detector address. A device tree and the device names shall be provided for in the GUI.</p>	
	<p>Import Export tool: The Access Control System AS shall provide a web based import and export interface to import cardholder master records from a separate database during installation, or to export the master records for further</p>	

RESTRICTED

	use by another application in CSV format.	
	<p>Areas</p> <p>The Access Control System shall provide the ability to define and manage arbitrary logical areas within the premises. These could be single rooms, groups of rooms, entire floors or parking areas.</p>	
	<p>Access Sequence Check</p> <p>There shall be an access sequence check provided, allowing authorized cardholders to enter an area only when they have swiped their card at the neighboring area.</p>	
	<p>Threat Level Management:</p> <p>At least 15 different threat levels can be pre-configured for instant activation in case of emergency. A threat level is activated by a threat alert. A threat alert can be triggered in one of the following ways:</p> <ul style="list-style-type: none"> • By a command in the software user interface • By an input signal defined on a local access controller, for instance from a push button or a fire panel. • By swiping an Alert card at a reader <p>Threat alerts can be cancelled by the UI command or hardware signal, but not by alert card.</p>	
	<p>Swipe Ticker:</p> <p>An application can be configured within the Map view that displays the last 10 minutes of access events in a dynamic scrolling list. The operator can easily pause and resume the display.</p> <p>Each record in the list contains details of the event and the credential used, for example:</p> <ul style="list-style-type: none"> • The name of the cardholder and their stored photo, for visual confirmation of identity. • A time stamp. • Company and/or department name • The entrance and the reader at which the credential was used • An event category: Green- Access event Yellow- Incomplete access Red- Invalid access 	
	<p>Random screening:</p> <p>The Access Control System shall be able to perform an additional security check by the officer on duty. The readers are easily set to random screening mode by checking a checkbox and setting the frequency. If the randomizer selects this cardholder for extra</p>	

	<p>security checks. The card is blocked throughout the whole system, until the block is manually removed. Once the screening is done, security can unblock the card or card can be unblocked after certain pre configured time.</p>	
	<p>Blocking cards: The Access Control System shall allow the blocking of cardholders as configured in the system, for example a defined validity period.</p>	
	<p>Alarm Handling and Management: The Access Control System AS shall provide a wide range of standard events. The following events, but not limited to, shall be supported:</p> <ul style="list-style-type: none"> • Card unknown • Card not authorized • Card outside time profile • Card anti-passback • Access timeout • Door open time exceeded • Door opened unauthorized • Door blocked • Tamper alarm controller • Tamper alarm reader • PIN code error • Duress alarm code • Access denied • Wrong card version • Card blocked • Card blacklisted • Card out route • Guard tour alarms • Random screening • Other individual alarm extensions <p>The Access Control System shall provide a wide range of standard events. All events are pre-configured in 4 alarm groups “hold-up”, “alarm”, “warning”, “maintenance”. The incoming alarm or event message shall provide, but not limited to, the following information:</p> <ul style="list-style-type: none"> •Alarm date and time •Alarm status •Alarm location <p>The Access Control System shall provide the operator a simple and efficient way to handle any incoming alarms. The operator shall be allowed to switch between all alarms or events messages.</p>	

RESTRICTED

	The Access Control System operator shall also be able to send remote commands or activate controls manually from the workstation when requested.	
Accessories	Should be mention and quoted as per requirement	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

31. Turnstile Gate with RFID Access control Module		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably TURNSTILES.us /ZKTeco USA/Astrophysics / Garret/Boon Edam / Turn Star / Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Product Size:	To be mentioned	
Passage Direction:	Single directional/Bi-directional	
Throughput Rate:	20~30p/m	
Reaction time	2.0s	
Power Supply	AC100-240V	
Working Environment:-	10-70 °C	

32. Walk through gate		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Astrophysics / Garret/Boon Edam / Turn Star / Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Detection Zones	33 zones (left, right and center); visual and audible alarms with a built-in dry contact alarm relay	
Multi-Unit Synchronization	Synchronization with wired AC power lines or with manual frequency selection for wireless operation	
Visual Displays	LED zone indicator lights on both panels. Pace lights on entry side only, with intuitive images	
Access Control	Eight-button keypad with numerical codes. Keypad lock to control access and to enable/disable the keypad.	
Passageway Interior Size	Width 30" (0.76 m) Height 80" (2.03 m) Depth 23" (0.58 m)	
Overall Exterior Size	Width 35.5" (0.90 m) Height 91.5" (2.32 m) Depth 6.25" (.16 m)	
Operating Temperatures	-4° F (-20° C) to +149° F (65° C); Humidity to 95% non-condensing.	
Power	Fully automatic 100 to 240 VAC, 50 or 60 Hertz, 45 watts; no rewiring, switching or adjustments needed	
Regulatory	Meets international airport standards such as TSA, ECAC, STAC, AENA, CJIAC, DFT. Meets	

RESTRICTED

Information	additional standards and requirements such as USMS, NIJ-0601.02, NILECJ. Meets Electrical Safety and Compatibility Requirements for CE, FCC, CSA, IEC, ICNIRP, IEEE.	
Weatherproofing	Meets IP 55, IP 65, IEC 529 Standard for moisture, foreign matter protection	
Construction	Attractive scratch and mar-resistant laminate. Detection Heads and Support: heavy duty aluminium.	
Control Outputs	Solid state switches (low voltage AC or DC) for operating external alarms and control devices	

33. CCTV Surveillance System

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell or Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
	All the active components quoted for Access control system must be from a single OEM	
Physical Dimension	Please Mention	
NDA compliant	Should be NDA Compliant	
Resolution	Minimum 5 MP	
Image sensor type	Should have 1/2.7"	
Max. frames per second (fps)	Minimum 30@5MP	
Indoor / outdoor	Outdoor	
Quantity	a). Bullet IP Camera-32Nos	

RESTRICTED

	b). PTZ IP Camera-6Nos c). Dome IP Camera-10Nos	
Built-in IR lighting	Should have 30 Meter / 98 Feet	
Wide Dynamic Range	Should have 120db	
ONVIF conformant	Should be ONVIF Conformant	
Power over Ethernet (PoE / PoE+)	Should have PoE Port	
Advanced Features		
Compression	Should have H.265, H.264, MJPEG	
Multi-streaming	Should have 3 streams	
Intelligent Dynamic Noise Reduction	Should have Intelligent Dynamic Noise Reduction	
Intelligent streaming	Should have Intelligent streaming	
Alarm triggering		
Video Analytics - pre-installed	Should ve IVA Pro Buildings	
Tamper detection	Should have temper detection	
Sensitivity		
Min. illumination day mode (color)	Should be 0.14 lux	
Min. Illumination night mode (B/W)	Should be 0 lux	
Lens		
Varifocal	Should be varifocal	
Automatic Varifocal (AVF)	Should be Automatic Varifocal (AVF)	
Iris control	Should have DC-iris	
Focal length from	Minimum 3.3 mm / 1.30 Inch	
Focal length till	Minimum 10.2 mm / 4.02 Inch	

RESTRICTED

Horizontal Angle of View (HAoV)	Minimum 30.1° x 101.4°	
Min. view angle (H)	Minimum 30.1°	
Min. view angle (V)	Minimum 21.8°	
Max. view angle (H)	Minimum 101.4°	
Max. view angle (V)	Minimum 69.6°	
Tilt angle	Minimum 0~85	
DCRI distances (in m with 100 lux illumination)		
Detection	Minimum 42m-193m	
Classification	Minimum 17m-77m	
Recognition	Minimum 9m-39m	
Identification	Minimum 4m-19m	
Storage		
(micro)SD-card slot	Should have (micro)SD-card slot	
Capacity of SD Card	Should have 64GB micro SD card in each camera from day one.	
Direct-to-iSCSI	Should able to connect with direct-to-iSCSI	
Housing		
Weather rating	IP66	
Vandal resistant	IK10	
Operating temperature	-30C to 50C (-22F to 122F)	
Network Video Recorder	Quantity-02	
Processor	Minimum Intel Xeon Processor E3-1275 V3 (8 MB Cache, 3.5 GHz) processor	
Cache	Minimum 8 MB Intel Smart Cache	

RESTRICTED

Memory	Minimum 8 GB, DDR3-1666 ECC UNB (1 x 8 GB)	
HDD slots	Minimum 16 slots, 3.5 in. SATA storage trays	
HDD for video	Minimum 8TB/HDD Total Number of HDD 16Nos.	
SSD for OS	Minimum 2 x 120 GB SSD drives in RAID-1 configuration	
OS	Should have Windows Storage Server 2012 R2 license built in	
RAID support	Should support RAID-5 / 6	
Protocol	Should be iSCSI	
B/W capacity	Minimum 550 Mbit/s	
Network	Should have dual Gigabit LAN (teamed)	
Hot swappable HDDs	Yes	
Hot swappable power supply, fans	Yes	
65" LED Display for CCTV view.	2Nos	
Power Consumption	Please mention	
Power Input	Please mention	
Form Factor	Should be rack mountable. Please mention	
USB Ports	Should have Front: 2 USB 2.0 ports, Rear: 2 USB 2.0 ports, 2 USB 3.0 ports	
Dimensions (H x W x D)	Please mention	
Weight	Please mention	
Operating Temperature	Please mention	
Non-operating Temperature	Please mention	
Operating Relative Humidity	Please mention	
Non-operating	Please mention	

RESTRICTED

Relative Humidity		
Quality	This product shall be manufactured by a firm whose quality system is in compliance with the I.S. /ISO 9001/EN 29001, QUALITY SYSTEM.	
SNMP	Should support Simple Network Management Protocol is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.	

34. Raised Floor (Quantity: approx4000 sft)		
Brand	To be mentioned (Preferably Arctiv/ RHGx600/ Maro or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Total Floor Area	Bidder will proposed as per drawing & requirement	
Features of Solid Panel	1.Fiber-reinforced Calcium Sulphate Panel	
	2.Panel thickness: 32 mm minimum	
	3.High pressure laminate: 1.0mm HPL minimum	
	4.Uniform Load: 23000N/m ²	
	5.Point Load/Concentrated load: 450KG	
	6.Rolling Load: 4450N/10 times	
	7.Panel Weight: 18 KG approx	
	8.Concentrated Load: 450 KG	
	9.The panel shall meet the high requirements regarding dimensional accuracy acc. to RAL-GZ 941/EN12825 to guarantee high air tightness. High air leakage rate requirements are guaranteed as well.	
	10.Panel should be fire proof, dustproof and corrosion resistant	
	11.Panel size: 600 x 600 mm	
	12.Accessories: Pedistal, stringer, gasket etc.	
	13.Raised floor panels/tiles must be Anti-static with 1.5 Ft. high steel understructure.	
	14.The legs of the raised floor are all separate from each other	
	15.All legs of the raised floor are connected with earthing cable.	
	16.To pass the electric cable from the rack to the power socket under the raised floor proper cap to be used in the raised floor tiles.	
	17.The raised floor should be installed in such a way that the PAC for down flow and the proposed water	

RESTRICTED

	detection system can be installed properly and can be serviced easily afterward.	
Features of Perforated Panel	1.Perforated steel panels designed for static load shall be interchangeable with standard field panels and capable of supporting concentrated loads with at least the load carrying capacity as the standard panels.	
	2.Panels shall have 58% or higher free air flow with Damper	
	3.Panel shall have damper added to control the airflow (optional)	
	4.The panel carrier plate consisting of a welded tube frame and must be conductive powder coated	
	5.Panel should made of non combustible materials	
	6.Panel size: 600 x 600 mm	
	7.Panel thickness: 32 mm minimum	
	8.Concentrate load: 3650N	
	9Load bearing capacity: 16,100 N/m2	
	10.Accessories: Pedistal, stringer, gasket etc.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

35. Data Center Floor insulation (Approx 4000 Sft)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	To be mentioned	
Total Floor area	(Bidder will proposed as per drawing & requirement)	
Features	<ul style="list-style-type: none"> a. A closed- cell structure not prone to wicking b. Mould resistance c. Dust and fiber-free construction d. An in- built water vapour barrier e. Ease of cutting and fitting f. Durability and maintenance 	

RESTRICTED

BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

36.Dry wall & Paint Works		
Dry wall	Fire rated two layer Gypsum Board Partition	
	10" Thickness two layer Gypsum board partition work with first class fire rated gypsum board. Inside the board should use glass wool to protect fire. MS Metal frame with all necessary accessories.	
Total area	Bidder will proposed as per drawing & requirement	
Paint work	Epoxy paint for inside server room, power room wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: To be mentioned	
	Country of manufacture: To be mentioned	
	Approved colour of epoxy paint to wall/column of inside wall,of the server room, power room, etc of two coats over a coat of brand specified primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding by roller/ spray etc and printing with two coats of epoxy paint approved color over a coat of priming etc all complete as per direction	
	Normal Paint for noc room and other wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: Bangladesh	
	Country of manufacture: Bangladesh	
	approved colour of normal paint to wall/column of inside wall,of the NOC, staging, open area etc of two coats over a coat of brand specified primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding	

	by roller/ spray etc and printing with two coats of normal paint approved color over a coat of priming etc all complete as per direction	
--	--	--

37. Water Leak Detection System to cover Data Center floor (Server, MMR & Power rooms) all critical areas & points) embedded with Monitoring & Notification		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
General requirement	Water Leak Detection System to cover Data Center floor (Server, MMR & Power rooms) all critical areas & points) embedded with Monitoring & Notification	
Floor area to be covered	Bidder will propose as per design & requirement.	
Addl Features	<ul style="list-style-type: none"> a. should be able to detect the moisture bellow the raised floor. b. It should provide immediate warning after detecting the moisture and water. c. It should be Micro-Processor Based Control 	
	<ul style="list-style-type: none"> d. Monitors each zone independently. e. Provides subsequent alarming, no matter how many zones go into ALARM or FAULT. f. Identifies location, time & date of all ALARM and FAULT conditions. g. Alarming should be provided at-least via two or more of the below state method Audible Visual h. In-band and out-of-band methods indicating in the software console and/or in the Building management system. <p>Monitoring software should be provided with the system.</p> <ul style="list-style-type: none"> j. Each cable length should be 20 feet or higher. k. To provide the solution if any other component has to add it should be included and the price should be required. 	
BOM	BOM to be attached with technical compliance of each item	

RESTRICTED


Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

38. Lightning Protection System		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of manufacturer	As per Tender Specification Article no 20	
General Features	<ul style="list-style-type: none"> a. A lightning protection system includes a network of air terminals, bonding conductors, and ground electrodes designed to provide a low impedance path to ground for potential strikes. b. Required resistance <1 Ohm c. Grounding rods, inspection pit, lightning event counter have to be considered. 	

39. Rodent System		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Master controller	Bidder will offer advanced rodent repellent system considering as per drawing.	
Transducer	Bidder will offer transducer considering as per drawing.	
Wire bundle	Wire bundle	
Installation	Installation Material, Testing & Commissioning Charge	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

40. NOC with Gallery type seating arrangement		
Brand	To be mentioned	
Origin	As per Tender Specification Article no 20	

RESTRICTED

Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	To be mentioned	
Specifications of Display Panel	Please Specify	
Number of steps in gallery	02	
Number of seats per steps	04	
LCD panel size of the NOC room	(W:H)(20' X10')	
Number of display for the LCD panel	At least 15nos	
Size of each display for the LCD panel	55" or above (Preferably SAMSUNG) .	
Sample image		
Functionality Required	<ul style="list-style-type: none"> ➤ Linear and asymmetric ➤ Scheduled play ➤ Multiple aspect ratios ➤ Full HD on every screen ➤ Display multiple sources ➤ Display images across single or multiple screens ➤ HDCP support ➤ Image rotation ➤ Art wall (any angle) ➤ Remote monitor management <p>Live camera and PC feeds</p>	
Specifications of Central Server	Please Specify	
Specifications of individual video controller/Set Back	Please Specify	

RESTRICTED

Box		
Electrical and Network	All network and power connections (from Bus-bar) have to be provided.	
Infrastructure work	All infrastructure work (Brick, tiles, Iron work, interior etc as per attached sample image or vatted by the BNET acceptance committee .	
Chair	10number of comfortable chair with headrest	
Table	As required for 2 rows, 4person in each row	
Drawer cabinet	At least 8 set.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

41. Fork-lift for equipment Movement inside Data Center		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Load Capacity	Please Specify (Minm.5 Ton)	
Lifting Capacity	Please Specify (Minm7 Feet)	
Dimension	Please Specify	
Horizontal arm extension	Minimum 1000 mm	

Sample image		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

42. PA System		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
01X Controller	Public Addressable Voice Alarm System (PAVA)	
	Model/Part Number: Please mention	
	EN 54-16 certified and EN 60849 compliant	
	The controller can be used as a stand-alone system with up to six zones, or expanded to up to 120 zones using additional six-zone routers.	
	Up to eight call stations	
	One-channel or two-channel operation	
	Fully supervised system	
	Heart of the Plena Voice Alarm System	
	Six-zone system controller	

RESTRICTED

	Built-in 240 W amplifier	
	6 emergency and 6 business triggers	
	Approvals: Europe CE Declaration of Conformity, Poland CNBOP	
3 X Zone Call Station for Main amp zone		
	Model/Part Number: Please mention	
	Stylish six-zone call station for the Plena Voice Alarm System	
	Six zone selection keys, all-call key and momentary PTT-key for calls	
	Selectable gain, speech filter, limiter, and output level for improved intelligibility	
	LED indications for zone selection, fault, and emergency state	
	Call station extension provides seven additional zone and zone group keys	
	Approvals: Europe CE Declaration of Conformity	
3 X 07 Zone Plena Voice Alarm Keypad		
	Model/Part Number: Please mention	
	Seven zone selection keys	
	LED indications for zone selection	
	Up to eight keypads can be connected together	
	Approvals: Europe CE Declaration of Conformity	
3 X Power Amplifier for Each Zone (480W)		
	Model/Part Number: Please mention	
	480 W power amplifier in a compact housing	
	70 V / 100 V and 8 ohm outputs	
	The Amplifire Shall have Dual inputs with priority switching	
	100 V input for slave operation on 100 V speaker	

RESTRICTED

	line	
	The Amplifire shall Temperature controlled forced front to back ventilation, directly stackable.	
	The Amplifire shall have facility Mains, battery back-up and pilot tone supervision	
	Approvals: Europe CE Declaration of Conformity	
Plena Voice Alarm Router	As required	
	Model/Part Number: Please mention	
	Expand the voice alarm system with six zone	
	EN 54-16 certified and EN 60849 compliant	
	12 additional input contacts	
	Six volume override output contacts	
	Supervision within the Plena Voice Alarm System	
	Approvals: Europe CE Declaration of Conformity	
25 X 5W Premium Sound Cabinet Loudspeaker		
	Model/Part Number: Please mention	
	High-fidelity music and speech reproduction	
	Selectable 8 ohm, 70 V and 100 V inputs	
	Compact yet robust ABS enclosure	
	Supplied with adjustable mounting bracket	
	Complies with international installation and safety regulations	
	Approvals: Europe CE Declaration of Conformity	
3 X 10 W Horn Loudspeaker		
	Model/Part Number: Please mention	
	Up to 45 W (max. power)	
	Wide opening angle	
	Water- and dust protected to IP 65	
	Versatile mounting bracket	

RESTRICTED

	Approvals: Europe CE Declaration of Conformity	
PLE-SDT Plena Easy Line SD Tuner BGM source	As required	
	Model/Part Number: Please mention	
	MP3 playback from SD card and USB inputs	
	FM tuner with RDS, presets and digital control	
	Simultaneous operation of SD/USB-player and FM tuner	
	Separate outputs for digital source and FM tuner	
	Approvals: Europe CE Declaration of Conformity	
Fire Detection & PAVA System Integration Device		
	Model/Part Number: Please mention	
	Connection of peripherals with RS232 serial interface	
	Ready to go thanks to plug-and-play technology and pluggable terminal blocks	
	The System shall have facility Seamless Integration between PAVA and Fire Alarm System	
	Approvals: Europe CE Declaration of Conformity	
2X1.5m Cable		
	Brand: BRB/Partex	
	Origin: Bangladesh	
1 X 15U Server Rack	15U Server Rack	
Brand	TO BE MENTIONED	
Model	TO BE MENTIONED	
Origin	TO BE MENTIONED	
PVC pipe with Accessories		
	Brand: Poly/Bengal/RFL	
	Origin: Bangladesh	

RESTRICTED

	20 mm dia PVC pipe with related joints	
Installation	Supply, Installation, Programming , Commissioning of the System	
Instruction and other activities		
As built design	Bidder should provide a built-up design with details during implementation and FAT period	
Labelling	Printed labelling enclosed with each applicable item	
Others	Bidder should accommodate additional items if required during the implementation period.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

43. Wireless Powered Desktop Laminated Label Printer

Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Type	Barcode Label Printer	
Printing Method	Thermal Transfer	
Cutter	Automatic	
Max. Print Speed	60 mm/sec	
Paper/Media Types	TZe, HSe, FLe	
Tape Size	36mm	
Maximum Tape Width	36mm	
Memory	6MB	

RESTRICTED

Interface (Built-in)	USB, Wi-Fi, Serial	
Cartridge	Bidder will provide at least 50nos cartridge with this label printer.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

44. Dual-Sided Card Printer with ribbons & cards.

Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Type	Card Printer	
Print Speed (Black)	450cph	
Print Speed (Color)	140cph	
Power Source/ Power Consumption	90-132VAC and 190-264VAC RMS	
Ribbons	20nos of ribbons to be provided in day one.	
Card	100nos of ribbons to be provided in day one.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

45. Fire rated door for data center (Quantity: 2nos Single leaf(3'6"X7'), 6nos double leaf (5'0"X7')		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Feature		
Fire rating	for 120 Minutes, Conforms to IS3614 (PART-2)1992, BS476 (PART 20 & 22) and ISO834.	
Material:	Door Frames and Leaves are made from Galvanized Steel	
Door Leaves:	Constructed from 2.0mm thick galvanized steel sheet formed to provide a 48mm thick fully flush, double skin door shell with seamless welding joint all around. The internal construction of the door shall be specially designed with infill to give 2 hours fire rating.	
Infill:	All the doors will have Honey Comb Crafted Paper or equivalent infill.	
Vision panel:	Fire Rated glass vision panel	
Accessories	Hinge, bolt and screw: Fire rated Lock: Built in mortise lock Auto Door Closer: Default Push panic bar: built in	
Standards	UL Listed Fire door NFPA 251 Standard Test standard: Fire Door must be tested according to BS Standard	
BOM	BOM to be attached with technical compliance of each item	

RESTRICTED

Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

PASSIVE HARDWARE FOR NHQ DC

1. Server Rack with KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/ / Vertiv / Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1500 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	Ø 04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 1U Universal Horizontal Cable Manager	
	Ø 04 units 2U Universal Horizontal Cable Manager	
Vertical Cable Manager	At least 4 Vertical cable managers should be provided with each rack.	
Fixed trays/shelves	2 Fixed trays/shelves capable of caring at least 50 kg load, depth of at least 900 mm should be provided with each rack	

RESTRICTED

Sliding trays/shelves	1 Sliding trays/shelves should be provided with each rack	
Tool less Airflow Management	At least 20 U blank panel should be provided with each rack	
Blanking Panels		
Stabilization	Should be provided	
Rack Monitor	17" TFT rack mount APC/Vertiv/Arctiv or equivalent monitor which occupies only 1 U / 2U rack space	
	1 unit for each rack	
Integrated Keyboard and Mouse	Required with sliding functionality	
Power Distribution Unit (PDU) with built-in K-type transformer	Switched Rack PDU, 32A – At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
	Metered Rack PDU, 32A – At least 42 way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
KVM Switch	Switch that allows 2 users (one remote & one local User) single-point access and control of up to 16 multiple servers from a single console with 16 units KVM console cable and 16 units 1.5mtr cat 6 & 16 units 3mtr cat 6 patch cord	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each Rack to connect the servers/network/PDU equipment with the quoted rack.	
	02 units of C20 to industrial female (32A)	
	02 units of C19 to industrial male (32A)	
	02 units of C14 to industrial female (16A)	
	02 units of C13 to industrial male (16A)	
	04 units of C19 to C20 cable (16A, 3m).	
	10 units of C13 to C14 cable (10A, 3m).	
10 units of C13 to C14 cable (10A, 2m).		
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

2. Rack without KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1200 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 1U Universal Horizontal Cable Manager	
	04 units 2U Universal Horizontal Cable Manager	
Tool less Airflow Management	At least 20 U blank panel should be provided with each rack	
Blanking Panels		
Stabilization	Should be provided	
Power Distribution Unit	Metered Rack PDU, 32A – At least 42	

RESTRICTED

(PDU) with built-in K-type transformer	way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
	Switched Rack PDU, 32A– At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.-	
	02 units of C20 to industrial Male (32A)	
	02 units of C19 to industrial Female (32A)	
	12 units of C19 to C20 cable (16A, 3m).	
	10 units of C19 to C20 cable (16A, 2m)	
	10 units of C13 to C14 cable (10A, 3m).	
	10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

3. Automatic Voltage Regulator-300KVA		
Feature List	Feature Description	Bidder Response
Brand:	To be mentioned (Preferably Ortea/IREAM or equivalent)	
Model:	To be mentioned	
Country of origin:	As per Tender Specification Article no 20	
Manufacturing Country:	As per Tender Specification Article no 20	
Capacity:	300 KVA	
Input:		
System:	Three Phase	
Input voltage variation:	±15 %	
Input voltage range:	340-460 V	
Frequency:	50Hz ±5% or 60Hz ±5%	
Max input current:	As per design	

RESTRICTED

Output voltage:	400 V	
Rated output current:	As per design	
Efficiency:	>98 %	
Adjustment speed:	24 ms/V	
Control:	Servo motor	
Standard features		
Voltage stabilization:	Independent phase control	
Admitted load imbalance:	100 %	
Ambient temperature:	-25/+45°C	
Storage temperature:	-25/+60°C	
Max relative humidity:	<95% (non-condensing)	
Admitted overload:	200% 2min.	
Harmonic distortion:	None introduced	
Protection degree:	IP 21	
Overvoltage protection:	Class II output surge arrestors, Optimal voltage return through supercapacitors in case of black-out	
Dimensions WxDxH:	To be mentioned by the bidder	
Weight:	To be mentioned by the bidder	
Installation & Commissioning:	Installation, testing and commissioning with necessary accessories.	
MAF	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
Warranty:	3 (Three) years full warranty (onsite covering everything with parts and services);	

4. Modular Online UPS-100KVA/KW		
Feature List	Feature Description	Bidder Response
General Requirement	The vendor shall provide 2x100 KVA modular Hot Swappable UPS in (N+N) configuration. The power cabinet must be of 250 KVA each. Also, each power cabinet shall be consisting of multiple numbers of hot-swappable power modules.	
Brand:	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per tender specification, article 20	

RESTRICTED

Country of Manufacture:	of	As per tender specification, article 20	
Country of Shipment:	of	To be mentioned	
Capacity:		Minimum 100 KVA to be upgradable up to Min 150 KVA in a single cabinet.	
Module:		Each Module will be minimum 25KW Hot Plug and hot swappable function	
Number of Module:	of	To be mentioned	
Backup Time:		Minimum 30 min at 100 KW full load from two separate battery Bank Combinedly. Each battery bank shall capable to provide backup for minimum 15 minute at 100 KW full load	
Battery String(Bank):		Each UPS Shall have Minimum two (2) battery String /Bank /Cabinet with separate controller per string/Bank/Cabinet.	
Input Battery Voltage:		Selectable and Configurable	
Topology:		Modular, True Online Double Conversion with Distributed/ Decentralized Active Redundant Architecture	
Input Power factor:		Minimum 0.99 at full load	
Output Power factor:		1 or unity	
Input			
Input Wiring:		3Ph+N+PE	
Rated Voltage:		380/400/415Vac	
Voltage Range:		For loads <100% (-25%, +20%) <80% (-32.5%, +20%) <60% (-35%, +20%)	
Input Frequency:		40-70 Hz	
Total Harmonic Distortion:		THDi<3% for linear load, THDi<5% for nonlinear load	
Bypass			
Input Wiring:		3Ph+N+PE	
Rated Voltage:		380/400/415Vac	
Input Frequency:		50/60 ±2/4% (selectable)	
Input Feed:		Duel	
Output			
Output Wiring:		3Ph+N+PE	
Rated Voltage:		380/400/415Vac	
Frequency:		50 Hz / 60 Hz	
Waveform:		Sine wave (THDv<1% for linear load THDv<3% for non-linear load)	
Overload Capacity:		Inverter 124% continuous 125% overload for 10 min 150% overload for 1 min, Bypass 135% overload for long term <1000% overload for 100ms	
Crest factor:		3:01	
General Features			

RESTRICTED

Features of individual Modules of Modular UPS system:	Individual rectifier, inverter, Control Logic, Static Bypass, On/Off Switch and LCD Display.	
Redundancy, Fault tolerance and Fault Isolation	The UPS System shall Design for no single point of failure and should be driven by the different modules. It will not consist of any major component failure of which may cause the failure of all module's operations. It shall have fault isolation capability. True hot Swappable function.	
Controller:	Separate controller for each module.	
Alarm/Status Indicator	Alarm/Status Indicator for each module.	
Mechanical Bypass:	Central mechanical bypass switch	
Battery Connection:	Please mention	
Supported Battery Type:	Lithium-Ion and VRLA	
Efficiency (VFI):	Minimum 97 %	
Environment		
Protection rating:	IP 20 or Better	
Operating Temperature	0-40°C or To be mentioned	
Relative Humidity	To be mentioned	
Operating Altitude	Minimum 100 m without any derating	
Audible Noise	< 65dB or Better	
Communication		
LCD Display:	UPS shall have Minimum 6 inch (Diagonal) LCD Display for showing all necessary information Centrally. And individual LCD display for each module.	
Communication ports:	S-232/RS485 and SNMP	
Remote Monitoring & Management:	SNMP card with remote monitoring and management capability and compatible with Data Center Infrastructure Management System (DCIM)	
Standard:		
Safety:	IEC/EN 62040-1	
Electromagnetic Compatibility:	IEC/EN 62040-2	
Performance:	IEC/EN 62040-3	
Manufacturer Certification:	ISO 9001/ ISO 50001	
UPS Cabinet Weight & Dimension:		
Weight:	To be mentioned	
Dimension: WxHxD(mm):	To be mentioned	

RESTRICTED

Battery Specification		
Battery Type:	Lithium-ion	
Brand:	Please mention	
Model:	To be mentioned	
Country of Origin:	To be mentioned	
Country of Manufacture:	To be mentioned	
Nominal Voltage:	To be mentioned	
Battery Module:	The UPS shall have hot swappable battery module. Can be run with Lower/Higher number of Battery module.	
Battery Amp:	To be mentioned	
Number of Batteries:	To be mentioned	
Weight per Battery (Kg):	To be mentioned	
Battery Dimension:	To be mentioned	
Designed Life Time for Battery:	Minimum 15 Years	
Battery Cabinet:	External type best quality battery cabinet with circuit breaker, Controller with required electrical/electronic components, Battery Monitoring System and shielded battery module.	
Battery Cabinet Dimension:	To be mentioned	
Battery Monitoring System (BMS):	UPS Shall have Battery Monitoring System that capable to monitor individual battery voltage, Battery Impedance (Ohmic Value), temperature, health etc. with graphical report.	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

5. Floor Mounted Power Distribution System-100A (4 units) with Auto transfer Switch for Server room.

Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin:	As per tender specification, article 20	
Country of	As per tender specification, article 20	

RESTRICTED

Manufacture:		
Maximum Total Current Draw per Phase	100A	
Nominal Input Voltage	400V 3PH	
Input Frequency	47 - 63 Hz	
Rack Height	To be mentioned	
Features	Multiple distribution options (3-phase and 1-phase)	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Local and web-based monitoring: Status available to customers both in the data center and remotely	
	Current Monitoring: Monitors the aggregate current draw per power distribution unit.	
	Network management capability: Full-featured network management interfaces that provide standards-based management via Web, SNMP, and Telnet.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
	Modular design: Provides fast serviceability and reduced maintenance requirements via self-diagnosing, field-replaceable modules.	
Auto Transfer Switch (3-Phase) Features	Minimum 2 incoming capable of 100A current per phase from bus-bar.	
	1 outgoing capable of 100A current per phase to Floor Mounted Power Distribution System.	
	Built-in Web/SNMP management: Full-featured management via a Web browser as well as comprehensive management from a Network Management System.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 (Uptime Institute/epi) compliance in all aspects	
Warranty	Three (03) years full	

6. IT Power Distribution Module 3x1 Pole 3 Wire 32A (1-Phase 32A Industrial Socket)		
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	230V	
Output Connections	(3) IEC 309 32A (2P+E)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

7. IT Power Distribution Module 3 Pole 5 Wire 32A		
Brand	To be mentioned (Preferably Schneider/Vertiv/	

RESTRICTED

	Equivalent)	
Model	To be Mentioned	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	32A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 32A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

8. IT Power Distribution Module 3 Pole 5 Wire 63A		
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Nominal Input Voltage	400V 3PH	
Output Frequency	50 Hz	
Maximum Line Current per phase	63A	
Nominal Input Voltage	400V	
Output Connections	IEC 309 63A (3P+E+N)	
Features	Multiple distribution options: Superior design flexibility enables a wide range of customer requirements to be addressed.	
	System mobility: Power distribution units can easily be relocated to accommodate a changing data center environment	
	Safety: Enhance user safety with isolation at all touch points and with positive locking mechanisms that reduce the risk of accidental disconnection	
	Power monitoring: Measure and monitor power consumption and usage with branch circuit monitoring and output metering, which are included at no extra cost	
	Quick status information LEDs: Access status information about the performance of the Power Distribution Module	
	Toolless installation of breakers: Install factory-assembled Power Distribution Modules in under ten minutes - no tools are required	
	Regulatory Approvals: CE, VDE	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full	

9. Rack Automatic Transfer Switch for single corded equipment		
Brand	To be mentioned (Preferably Schneider/Vertiv/Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	To be mentioned	
Type	Automatic switching power redundancy to single corded equipment	
Form factor	Rack mountable horizontal 1U or 2U solutions	
Manageability	Network manageable through TCP/IP	
Transfer Time	Zero	
Capacity	At least 6 kW or higher	
LCD display for operating information	Should be inbuilt with the system.	
Ports	At least 6 ports or Higher	
Software Interface and	ATS Monitoring and Management Software and Ethernet interface from each ATS.	
	Provided software's functions should include monitoring and Controlling the ATS remotely through TCP/IP	
Firmware upgrades	On-the-fly firmware upgrades should be possible	
Event logging	Event logging with graphs should be possible in the proposed software	
Cables	12 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.	
	04 units of C20 to industrial female (32A)	
	02 units of C14 to industrial female (16A)	
	04 units of C19 to C20 cable (16A, 3m). 02 units of C19 to C20 cable (16A, 2m)	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

12. Transient Voltage Surge Suppression (TVSS)		
General Information		
Brand	To be Mentioned (Preferably Schneider/ Rayvoss / Equivalent)	
Model	To be Mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Operating voltage, current and frequency	To be mentioned	
Features	Microprocessor-based controller	
	Plug-in modules for easy replacement	
Visual Indication	To be mentioned	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3/rated-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

13. Signal reference grid system		
	1. A separate & complete SRGS is to be installed in accordance with applicable codes & standards for data center, MMR-01&02, Power room-01&02.	
	2. Separate SRG sub system for both MMR is to be design & combindly will be connected with earthing system.	
	3. Separate SRG system is to be design for server room (All Server racks)	
	4. Seperrate SRG sub system for both Power room is to be design & combinedly will be connected with earthing system.	
	5. Grid pattern of SRG will be followed the mesh system to secure floor pedestal	
	6. In SRG system proper copper strip, grounding clamp, UL listed bonding grids, low impedance raiser kit, BCF weld, BHO weld, Flat strip pedestal ground clamp, CPC pipe clamp are to be used.	

14. Data Center Earthing & Bonding system.		
Bonding	1. Proper bonding for data equipment rack, telecommunication backbone, power cabinets, is to be designed & installed.	
	2. Proper & separate bonding network for power equipment, server rack, cooling system has to be interconnected with separate earth termination/grounding system.	
	3. Bonding connection at all SRG mesh intersections & bonding between mesh & equipment is to be confirmed.	
Earthing	4. Earthing System: The signal reference grid (SRG) system to be implemented for datacenter.	
	5. Ground Resistance: The ground resistance has to be below 0.5 ohm.	
	6. General Requirement: All metallic object including cabinet, PDUs, Cooling system, raised floor etc. should be connected to grounding system.	
	7. For Rack/cabinet continuity	
	a. Racks should be assembled with paint piercing grounding washers, under the head of the bolt and between the nut and rack, to provide electrical continuity.	
	b. A full-length rack-grounding strip should be attached to the rear of the side rail with threadforming screws to ensure metal to metal contact.	
	8. For Rack/Cabinet Grounding: Larger bonding conductor to bond each rack or cabinet with the grounding strip to the data center grounding infrastructure(SRG System)	
	9. For Telecommunications Grounding Bar	
	a. Provision of larger conductor to bond the data center grounding infrastructure to the TGB.	
	b. Two hole copper compression lugs are preferred for vibration.	
	10. Telecommunications Bonding Bar	
	a. The TBB should be installed as a continuous conductor, avoiding splices where possible.	
	b. Avoid routing grounding/earthing conductors in metal conduits.	
11. Telecommunication Main Grounding Bus Bar		
The TMGB is to be bonded to the service equipment (power) ground, which connects to earth ground (the grounding electrode system)		
12 Supplier need to consider earthing meter installed to the separate earthing group for DC equipment(Present & Proposed data center)		
13. Warranty: The vendor shall provide 3 years warranty.		

13. Data Center infrastructure Monitoring Software (DCIM)		
Brand	To be mentioned (Preferably Schneider/Vertiv/Sunbird/Commscope/Equivalent)	
Model name	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
No of device license required	At-least 100 node license (If more no. of license is required to cover the full Data Center as per given requirement, have to be included)	
	If the proposed system is an appliance based, the appliance should be provided.	
Design Requirements:		
	All material and equipment used shall be standard components, regularly manufactured, available and not custom designed especially for this project. The data center infrastructure system, including the DCIM, shall previously be thoroughly tested as a system, and proven in actual use prior to installation on this project	
	The DCIM shall be installed on a physical server, or as a virtual appliance, with a specified HTTP or HTTPS connection to access the user interface (DCIM client), and standard TCP protocol connections for communications with the monitoring system	
	The DCIM system-level redundancy and load-balancing shall be provided using a server-level cluster setup. Up to 4 servers should be setup in a cluster to gain performance improvements	
	The DCIM shall enable vendor-neutral inventory management with real-time device failures and data shown within a data center physical layout. Graphical floor layout and rack elevation view shall be supported from Day 1	
	The DCIM tool shall provide location-based drill-down views providing a structured overview of data center locations, from a global to local view down to single assets.	
	A Power Usage Effectiveness (PUE) dashboard will provide information on daily energy use	
	Inventory report provides structured information on all rack-mount devices, organized by device type, age, manufacturer, and properties for quick overview of all current devices within a particular data center	
	The DCIM tool shall have a search capability to allow	

RESTRICTED

	data center operations to quickly locate a piece of equipment in the rack layout and floor layout.	
	The DCIM tool shall provide public web services API to allow third-party applications to access the inventory database, alarms and events, capacity and cooling analysis data, and PUE information	
	The DCIM shall provide provisions to predict the optimal location for physical infrastructure and rack-based IT equipment based on the availability and requirements of physical infrastructure capacity and user defined requirements such as redundancy, network, and business use grouping	
	The DCIM shall provide provisions to reduce stranded capacity and enable informed decision making and planning by proactively analyzing the impact of future moves, adds, changes before they occur, ensuring that the physical infrastructure provides the required space, power, and cooling capacity for current and future needs	
	The DCIM shall be capable of hosting additional add-on modules that allow a user to perform energy efficiency and energy cost management, inventory management, power and cooling capacity management, change management, IT optimization, IT power capping, server access (software Keyboard Video Mouse or KVM), dynamic cooling control and mobile data center management	
	The DCIM shall provide read-only smart phone applications to get a high level status of the data center operations and KPI	
	The DCIM shall be capable of integrating with additional plug-ins that supports Cisco UCS Manager, HP OneView, Vigilent dynamic cooling control, BMC Remedy ticketing system, Microsoft System Center Virtual Machine Manager 2008/2012, HP uCMDB, and VmwarevCenter, etc.	
DCIM Operation	The DCIM software shall provide the methodology to create visual view of the data center floor layout, and the racks view and the equipment within, and manage network connectivity. This module shall also map the alarms to the appropriate device on the floor layout. The DCIM software shall support the following capabilities -	
	1. Floor Layout	
	A. The DCIM tool will have the capability to add locations and rooms of different types to the data center model to represent the actual physical enterprise infrastructure.	

RESTRICTED

	B. The DCIM tool will have the capability to configure a bird's eye view of the room layout to ensure the layout in the data center model accurately represents the real-world physical environment of the room. This includes any physical attributes of the room such as size, shape, doors, windows and walkways.	
	C. The DCIM tool will have the capability to see multiple rooms in a layout pane at the same time allowing a user to compare or drag equipment between them – for modeling.	
	D. The DCIM tool will have the capability to export the complete or filtered data center inventory into a delimited file (.csv file).	
	E. The DCIM tool will have the capability to render the floor layout in both 2D and 3D view.	
	F. Ability to import an AutoCad (.dwg) floor drawing and display the floor layout. Each layer can be toggled on or off. Rooms can be created based on wall detection on the AutoCad drawing.	
	G. Ability to export the Floor Layout to AutoCAD format (.dwg). Each overlay and the information in the overlay must be stored in individual layers.	
	H. Ability to export the Floor Layout to the following picture formats: BMP, JPG, PNG and SVG.	
	I. Ability to export the Rack View to the following picture formats: BMP, JPG, PNG and SVG.	
	J. Ability to copy/paste equipment on the floor, such as racks, PDUs, UPS and cooling units as well as equipment in the racks, such as servers and patch panels. You can	
	K. copy/paste individual pieces of equipment or multiple items, such as a rack and its contents.	
	2. Multi-tenant Data Center Support	
	A. Ability to create cages and auto-detect cage area in square meters or square footage.	
	B. Ability to create cages automatically from AutoCAD drawing through cage selection and wall detection.	
	C. Ability to assign customer to data center asset including rack mounted equipments, racks, cages, etc.	

RESTRICTED

	D. Cages, racks and servers are color coded based on sales status (closed, reserved, internal, and open).	
	E. Ability to assign Contracted Power value to each cage, rack or server.	
	F. Ability to add power receptacles to each cage.	
	G. Show a legend on the floor view with information about how many racks are open, closed, reserved and internal.	
	H. Show a legend on the floor view with information about how much space is open, closed, reserved and internal.	
	I. Show a legend on the floor view with information about total room area, sellable space and space efficiency.	
	1. Rack elevation View	
	A. The DCIM tool will identify how much weight has been placed in a rack / room compared to the predefined load bearing capability settings of the rack.	
	B. Illustrate the weight of the equipment added to the rack in the rack layout compared to the maximum equipment loading capability of the rack.	
	C. Visualize status of network ports on equipment (used vs. not used).	
	D. Visualize network cables.	
	1. Network Management	
	A. The DCIM tool will be able to model the configured network connections and allows a user to setup new network routes between the configured equipment.	
	B. Network port properties will have the capability to be imported from a product catalog and/or will be user configurable.	
	C. Ability to configure network routes for selected network equipment in the layout, for example between a server and a switch or a switch and a switch. A route is defined as a connection from a piece of equipment (communication endpoint, such as a server or layer 2/3 network gear, such as a switch) to the first piece of equipment that is a communication endpoint or layer 2/3 network gear.	
	D. Ability to configure cable types and color code each cable type.	
	1. Product Catalog	

RESTRICTED

	A. The DCIM tool will be able to provide a product catalog that contains up-to-date floor and rack mounted data center equipment.	
	B. The DCIM tool will be able to allow a user to add floor and rack-mountable equipment to a rack, server room, electrical room or store room.	
	C. Ability to create an inventory bundle that combines multiple pieces of equipment in one building block.	
	1. Dashboard Key Performance Indicator (KPI) View	
	A. Provide a map view to monitor the data center operations in a quick overview, including any alarms in different locations and rooms.	
	B. From the map overview, one can drill down to locations > rooms > racks > servers for details or troubleshooting.	
	C. Display capacity KPIs for each data center in the map view. The KPIs should include the status of the Power, Cooling, U-space and Network utilization.	
	D. Power is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	
	E. Cooling is represented as the percentage of the available load (kW) that is utilized by the IT equipment in the location or room.	
	F. U-space is represented as the percentage of the available U-positions (U-pos) that is populated with equipment in the location or room.	
	Network is represented as the percentage of the available Network ports (ports) that is utilized by networking equipment in the location or room	
Data Center Operation: Capacity	The DCIM software shall provide capabilities to perform capacity planning, create capacity groups, perform power and cooling analysis as per the following details:	
	1. Capacity Planning	
	The DCIM software will provide provisions to recommend the best location for a server in the rack layout, utilizing available space, cooling, network and power capacity to optimize capacity utilization and avoid stranded capacity:	
	A. Impact simulation: Generates a list of equipment that would be impacted if the selected piece of equipment, e.g. a UPS or cooling unit, was to fail.	
	B. Measured Load: Display measured load data for UPS and racks in the floor layout that identify how much of each UPS or rack's maximum kW power is in use. This requires	

RESTRICTED

	communication to power monitoring devices or servers.	
	C. Measured Load: Displayed measured load data for cages in the floor layout that identify how much of a cage's contracted power is in use. This requires communication to power monitoring devices or servers.	
	D. Power Capacity: Ability to assign planned capacity for each rack and illustrates rack capacity consumption compared to the planned recommended values for that rack. Provide information such as remaining power, the amount exceeding the recommended capacity.	
	E. Power Path: Ability to model power connections between the equipment supplying and delivering power and the equipment requiring power. This includes power path from switchgear, UPS, main PDU with modular circuit breaker mapping, rack RPDU and to individual servers.	
	F. Power Path: Ability to export the power path to a comma separated file.	
	G. Rack U Space: Ability to monitor and display rack U space utilization of each rack.	
	1. Capacity Groups	
	Ability to model capacity groups that allows a user to group equipment's, placing it in groups of racks with similar power capacity requirements to match the IT equipment with availability needs and avoid stranded space, power, and cooling capacity. For example, group a set of high-density racks together for optimized power and cooling configuration.	
	3. Power Analysis	
	Ability to detect the following list of configuration issues regarding data center power configuration and provide recommended actions:	
	A. Connection has not been configured between PDU and power supply: A power connection is missing in the data center model from this PDU to the power supply from which it should receive power.	
	B. Equipment connected to this PDU draws more power than is supported by the power supply breaker: The breaker does not provide sufficient power to cover the power requirements of the equipment connected to that PDU.	

RESTRICTED

	<p>C. Equipment is connected to a rack PDU outside this rack: The power connection setup for this equipment is not optimum as it is setup to be supplied by a rack PDU that is not positioned in the same rack as the equipment.</p>	
	<p>D. Internal redundancy setup for UPS and group must match: The internal redundancy setup for the UPS and group does not match, for example N and N+1.</p>	
	<p>E. Rack is without rack PDU or a rack PDU is not powered: The rack is without rack PDUs or its rack PDUs are not connected to a PDU, remote distribution panel (RDP) or power panel.</p>	
	<p>F. The breaker configuration does not support rack's estimated load: The equipment in the rack draws more power than the breaker supports. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.</p>	
	<p>G. The input voltage setting required by the equipment is not available in current rack: In the data center model, the server's input voltage requirement cannot be supplied by the rack PDU in the rack.</p>	
	<p>H. The measured load exceeds the estimated load per phase designed for the rack: Connected devices in the rack use more power than the estimated load per phase in the rack shall be indicated in the data center model.</p>	
	<p>I. The measured load exceeds the total estimated load configured for the rack: Connected devices in the rack that use more power than the total estimated load in the rack shall be indicated in the data center model.</p>	
	<p>J. The measured load of the UPS exceeds the total estimated load of the connected equipment: Devices connected to the UPS use more power than design capacity or they have not been assigned to the correct UPS in the data center model layout to correctly represent the physical infrastructure. In case of 3 phase equipment, the problem shall be indicated even if the measured value is only too high for one of the phases.</p>	
	<p>K. The phase configuration for the connected server is not supported by the rack PDU: The phase connection configured for this server is not valid. This message will occur if a power connection had been configured to this server but subsequently changes have been</p>	

RESTRICTED

	made to the phase configuration.	
	L. The Rack PDU output voltage setting does not match the output voltage of the connected PDU / Power Panel: The power connection is invalid because the voltage required by the rack PDU is not available from the power distribution component.	
	M. The server must be supplied from the same phase from both distribution units: The redundancy setup requires identical phase distribution setup for A and B feed.	
	N. The UPS in the layout does not supply enough power to match the configured load of connected equipment in the layout: The load of the equipment connected to the UPS is higher than the load that the UPS can supply. In case of 3 phase equipment, the problem shall be indicated even if only one of the phases is overloaded.	
	4. Cooling Analysis	
	A. The DCIM software shall be able to calculate cooling performance of data centers in real-time with CFD-like simulation, provide calculated inlet and exhaust temperatures per rack plus capture index (percentage of heat captured by cooling devices) per rack.	
	B. Ability to present the calculation results visually in the floor layout.	
	C. Ability to alarm cooling configuration issues and provide recommended actions. For example, a room has no perforated tiles for the Computer Room Air Conditioning (CRAC) unit airflow (one or more CRACs have been added to the floor but no perforated tiles have been added), or there is no perforated tile airflow (one or more perforated tiles have been added to the room but no CRACs have been provided to supply any airflow).	
	D. 2D plenum airflow and pressure view: Provide a 2D under-floor plenum view that shows airflow vectors and Cubic Feet per Minute (CFM) based on the height of the raised floor, the placement and type of perforated tiles and cooling devices. When a cooling unit or a perforated tile is moved around, the flow vectors and airflow CFMs shall update instantly.	

RESTRICTED

	E. 3D temperature and airflow view: Provide a 3D view showing max/average inlet/return temperature and airflow above the raised floor. Calculate velocity vector and temperature in real-time (seconds) to allow customers to try what-if scenarios. Ability to slide the temperature and velocity plane in all three dimensions.	
	F. Ability to simulate failure of one or more cooling units and examine impacts to IT equipment.	
	G. Ability to map temperature sensors to rack elevation or anywhere in the data center 3D space and draw the 3D measured temperature map based on the measured data.	
	5. Integration with 3rd Party Software	
	A. The DCIM software shall support integration with Cisco UCS manager to retrieve real-time power measurement data for blade servers and display them. In addition, it should support automatic power capping Cisco UCS chassis based on rack PDU breaker setting to safe guard rack PDU breakers.	
	B. The DCIM software shall support integration with VmwarevCenter and Microsoft System Center Operations Manager (SCOM), Virtual Machine manager to retrieve virtual machine information and map them to physical servers.	
	C. The DCIM software shall support integration with HP Universal Configuration Management Database (uCMDB), pushing IT asset data such as network, server devices and properties to the DCIM software.	
	D. Ability to support two-way data exchange between the DCIM software and a broad range of systems, such as CMDDBs, asset management systems, and building management systems using Extract, transform and load (ETL). Based on the ETL system, it is possible to develop custom solutions, integrating DCIM with a broad range of data sources.	
Data Center Operation: Energy Efficiency	The DCIM shall provide the following functionality from the data center Energy Efficiency point of view	
	1. The DCIM tool will provide current and historical Power Usage Effectiveness (PUE) values and full insight into current and historical energy efficiency.	
	2. It will present how much power is devoted to driving the installed IT-equipment compared with the total facility consumption.	

RESTRICTED

	3. Identify efficiency losses and enables improved PUE at the subsystem level.	
	4. Provide insight into energy losses and cost of energy at the subsystem level, providing details of which subsystem draws the most costs.	
	5. The DCIM tool will have a web-based dashboard view which includes efficiency data on current and historical PUE, as well as detailed subsystem cost analysis.	
	6. The DCIM tool will provide a report on current and historical PUE values.	
	7. The DCIM tool will provide energy efficiency analysis, PUE and DciE (Data Center infrastructure Efficiency) reporting.	
Data Center Operation: Change	The DCIM shall provide the following change management functionality to keep track of additions, movements, maintenance or deletions in a data center:	

14. Controlled electric lighting system (Electric lighting & Emergency Lighting)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Features		
Data Center Lighting & cabling	The data center automatic & manual lighting system with required cabling is to be design & installed by bidder. Lighting & interior design must be vatted from BNNET acceptance committee.	
Emergency Lighting Control	When the normal AC power fails, the emergency lighting system should sense the power failure and immediately switches to the emergency mode, illuminating more than 5 lamps at a time.	
	When AC power is restored, the emergency lighting system should returns to the charging mode until the next power failure	

RESTRICTED

No of Emergency Light	To be mentioned	
Central Control Panel	The central control panel should include all the power lighting and also the emergency lighting for allowing monitoring and control of Data center lighting system.	
Total Floor Area	As per drawing	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

15. Electrical Works

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Electrical DB Panels & DB Accessories		
	Supply & installation of Electrical Panels housed in 2.0mm standard sheet steel enclosure type tested, fixed Type, compartmentalized, totally enclosed, free standing, Floor mounted type, dust and vermin Proof, duly wired up and ready for installation at site. All MCB, MCCB & ACB should be Ics 100% Icu. The boards are designed and constructed in accordance with IEC61439-6. Busbars and other live parts are spaced and insulated in accordance with IEC standard. All	

RESTRICTED

	DB should C911:C925	
	<p>The DB system should have following features:</p> <ul style="list-style-type: none"> a. Factory assembled power distribution module with breaker position monitoring. b. No rear access c. Network management via web interface, SNMP, modbus and other appropriate interfaces. d. Compatible with Tier -3 data center. e. Self diagnosing module and tool less module replacement f. Output metering and branch circuit/current monitoring. h. Local access display interface 	
	Technical Description	
AVR Output DB-01	<p>Bidder will design & proposed required DB for AVR, Online UPS, HVAC, FMPDU, others utility load as per attached. During design bidder will consider appropriate bus bar, breaker, protection devices, monitoring devices for SCADA/DCIM monitoring.</p>	
AVR Output DB-02		
MDB-01		
MDB-02		
HVAC DB-01		
HVAC DB-02		
SECURITY DB-01		
SECURITY DB-02		
UPS O/P DB-01		
UPS O/P DB-02		
BOM		

RESTRICTED

Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

16. Power Cabling and Others related works

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably BRB/ Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Cable Requirements	Bidder's has to quote cabling for complete Data Center.	
	All connection of UPS, AVR, RACK and other electric items (approx. 10 Nos. Rack) inside the data center through IT Power Distribution Modules.	
SLD Diagram	Bidder has to provide Complete SLD starting from Sub-station to IT load	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

17. Power Cable Ladder		
Feature List	Feature Description	Bidder Response
Brand	To be mention	
Model	To be mention	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturing	As per Tender Specification Article no 20	
Type	Metal Steel/Stainless Steel Mesh Type Electrical ladder	
Cable ladder size	width 12"	
Height	Approx. 2"/Customized	
Materials	U Steel cable ladder with electro zinc plated treatment. Thickness: Min.1.6 mm and average load of more than 200KG per meter.	
Color	Powder coating White or Silver or Siemens Gray	
Installation material	Thread Rod/Hanger (max 3'), Flat BAR, Clump, Royal Bolt, Screw, Saddle, bending/L-shape, T-Shape etc. for hanging/vertical /Horizontal area both the overhead and under raised floor	
Power Cable Tray	Cable Tray	

18. Electrical Switch Sockets		
Feature List	Feature Description	Bidder Response
Electrical Switch Sockets	Brand: To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturing	As per Tender Specification Article no 20	
Industrial Socket		

RESTRICTED

32A SP	Supply and installation of imported 40/32/20A, 3-pin, 250V, industrial 3 pin socket outlet from foreign made suitable for 3 pin plug including the box complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge	
	Supply and installation of imported gang switches& socket and wall boxes complete with all other necessary accessories and connections everything complete as per drawing, specification and instruction of the Engineer-in-charge. The wall boxes may be locally made of 18SWG galvanized steel sheet including earthing block. (Maximum Current 13 Amps)	
	3-Pin wit 2 pin socket	
Switch for Light	Supply and installation of imported 13A, 220V, combined switched socket outlet including the box, cover plate with necessary galvanized machine screws, earthing block complete with necessary connections as per drawings, specifications and direction of the Engineer-in-charge. The box may be locally made of 18SWG galvanized sheet steel. Maximum Current 10 Amps	
	3 Gang Switch	
	4 Gang Switch	
	2 Gang Switch	
Lighting System	Supply of ceiling surface/concealed mounted light fixture complete with energy saving LED light, best quality lighting shade with mounting kit and all other necessary materials as per drawing, specifications and direction of the Engineer-in-charge.	
	Recessed Ceiling Luminaires, Series for LED panel light 2'x 2' with hanging accessories	
Emergency light with battery back up		
Brand:	Any international Reputed Brand	
Model:	To be mentioned by bidder	

RESTRICTED

General Features	Emergency light luminaire	
	Input: 220VAC +/- 10% 50 Hz 1 phase	
	Bulbs: 2 x 9W & 12 W SMD LED super wide beam 90 Deg.	
	Lamp: Aluminum heat sink body and plastic diffuser 180 Deg. Adjustable legs	
	Automatic solid-state system	
	Constant current charger	
	10-12 Hours charging duration	
	Battery Nickel Metal hydride (Ni-MH)	
	Battery protection: Low voltage cut off	
	System protection: high voltage cut off	
	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: front cover 1.5mm electro-galvanized steel sheet with epoxy powder coated and stove enamel	
	Operation temperature: 10 Deg. - 40 Deg.	
	IP rating: IP 20	
	Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)	
TIS.1102-2538 (self-contained emergency light Luminaries)		
Emergency Exit Sign	Wall and ceiling mounted	
Brand	Any international Reputed Brand	
Model	To be mentioned by bidder	
General Features	Input: 220VAC +/- 10% 50 Hz 1 phase	
	Lamp: SMD Surface mount	
	Automatic solid state system charger	
	Constant current charger	
	10-12 Hours charging duration	
	System protection: high voltage cut off	

RESTRICTED

	Safety features: AC fuse-protection of 220V AC input, DC fuse protection of battery charger	
	Construction: Electro-galvanized steel sheet 1mm & front plate 1.5mm epoxy powder and stove enamel coated anti-rust corrosion proof	
	ISO green legend	
	Certification: TIS.1955-2551 (Lighting and similar equipment : radio disturbance limits)	
	TIS.1102-2538 (self-contained emergency light Luminaries)	
Electrical Accessories	Accessories: Lugs, Heat Shrink, Cable tie, Screw, GI wire, Royal Plug, Royal Bolt, Clump, PVC Tape, Masking Tape, Rivet, High Quality nylon Fastener etc.	

19. Precision Air Conditioner (PAC)_DX for Server Room

Products Names/Items	Description of requirements	Bidder Response
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 40 kW	
Total sensible capacity	Minimum 40 kW	
Net Total Capacity	To be mentioned	
Net Sensible Capacity	To be mentioned	
Air Flow (Indoor)	To be mentioned	
Air Flow(outdoor)	To be mentioned	
Ambient Temperature	45 °C	
Fan Technology	EC Fan Technology	
Electrical power consumption	To be mentioned	
Energy Efficient Ratio (EER)	To be mentioned	

RESTRICTED

AER	To be mentioned	
Total power consumption	To be mentioned	
LpA (2m free field)	Indoor: 65.4 dB(A)	
LpA (5m free field):	Outdoor: 57.9 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50%	
Altitude above sea level:	100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 3 (three)	
Heat rejection	To be mentioned	
Condenser capacity	To be mentioned	
Compressor type	Scroll Type	
Expansion Valve	Electronic	
Electrical Heating	To be mentioned	
Steam humidification	To be mentioned	
Refrigerant	R407C	
Number of refrigerant circuits	Minimum 2 (two)	
Compressor:	Minimum 2 (two)	
Filter	To be mentioned	
Controller	a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
	b) Controller based Sequencing Facility c) water leak detector	
	c) Auto Shutdown by external fire alarm	
	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	
Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen,	

RESTRICTED

	Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

20. Precision Air Conditioner (PAC)_DX for Power Room

Description	Required Specification	
Brand	To be mentioned (Preferably Vertiv/Stulz or Equivalent)	
Model:	To be mentioned	
Country of Origin :	As per Tender Specification Article no 20	
Country of Manufacturer & Shipment:	As per Tender Specification Article no 20	
Cooling type	Air cooled	
Unit configuration Type	Down Flow.	
Total capacity	Minimum 14.8 kW	
Total sensible capacity	Minimum 12.9 kW	
Net Total Capacity	Minimum 14.1 kW	
Net Sensible Capacity	Minimum 12.2 kW	
Air Flow (Indoor)	Minimum 3,600 m ³ /h	
Air Flow(outdoor)	Minimum 10,600 m ³ /h	
Ambient Temperature	42 °C	
Fan Technology	EC Fan Technology	
Electrical power consumption	Maximum 3.6 kW/Compressor.	
Energy Efficient	3.44 kw /better	

RESTRICTED

Ratio (EER)		
Total power consumption	Maximum 4.3 kW	
LpA (2m free field)	Indoor: 56.2 dB(A)	
LpA (5m free field):	Outdoor: 51.1 dB(A)	
Return air temperature	24-26 degree Celsius	
Supply air temperature	14-16 degree Celsius	
Return air relative humidity	50%	
Altitude above sea level:	100 m	
Fan type:	To be mentioned	
Number of Fan	Minimum 1 (one)	
Heat rejection	18.6 kw (per compressor)	
Condenser capacity	18.6 kw each condenser	
Compressor type	Scroll Type	
Expansion Valve	Electronic	
Electrical Heating	9 to 18 kw or more	
Steam humidification	8 to 15 kg	
Refrigerant	R407C	
Number of refrigerant circuits	Minimum 1 (one)	
Compressor:	Minimum 1 (one)	
Filter	To be mentioned	
Controller	a) Microcontroller based recording at least 200 alarms with time & date and Temperature and humidity recording data points at least more than 1000.	
	b) Controller based Sequencing Facility c) water leak detector	
	c) Auto Shutdown by external fire alarm	
	d) Advanced Display System for Graphical Display and BMS connectivity	
Synchronization Requirement	PAC must be capable of running in Synchronization mode	
Dimension	a) Indoor (H x W x D): To be mentioned	
	b) Outdoor (H x W x D): To be mentioned	
Weight	a) Indoor (Kg) : To be mentioned	
	b) Outdoor (Kg): To be mentioned	
Certifications	Updated ISO Certification and EC Certification	
Voltage	400V/50Hz/3Ph/N/PE	
Installation	Installation and Commissioning should be done by OEM certified Engineer.	
Installation with all accessories	All installation accessories including a) extra power cable, b) Indoor Base, c) Outdoor Base, d) Oxygen,	

RESTRICTED

	Acetylene gas for welding, e) Nitrogen for leak test, f) Refrigerant, g) Indoor- Outdoor Cable, h) PVC Pipe, i) GI Pipe, h) Fittings (Copper, PVC & GI) etc.	
Support	Quarterly machine condition check, Servicing of units including on demand support Service.	
Declaration of spare parts availability	Vendor must provide surety that spare parts will be available for at least 10 years. In this regard vendor should make a contract with OEM.	
	Bidder must have minimum 10 years' experience in proposed brand PAC supply, Installation & Maintenance in Bangladesh, must be submitted proper evidence with the bid documents.	
	Manufacturer Authorization Form issued by OEM must be submitted with the Bid documents.	
	Distributorship Certificate must be submitted along with Bid documents.	
Warranty	3 Years	

21. VESDA System (Very Early Smoke Detection Aspirating) for DC Server & Power Room with Uptime compliance Zone separation

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Honeywell / Eaton / Xtralis / Bosch / Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Require Features		
Capacity	The proposed solution should be for Approx 750 sqft. Floor space.	
	The total electric load will be calculated for 10Racks where each Rack will consist of 5KW load (avg.)	
Additional equipment	Control panels.	
	Releasing devices	
	Remote manual pull stations	
	Corner pulleys	
	Door closures	
	Pressure trips	

RESTRICTED

	Bells and alarms	
	Pneumatic switches	
	Good to have TCP/IP base remote control capability from Day 1.	
Fire Detection System	Automatic detection for early warning of fire.	
	Should be able to identify different types of smoke.	
	Smoke detectors for gas discharge.	
	The detection circuits should be configured using coincidence or independent inputs.	
Other	If any other components have to be added to design and install the solution To be mentioned and quote the same.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

22. Automated Fire Suppression System for NHQDC Server & Power Room

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Name of the GAS agent	NOVEC-1230	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	

<p>Country of Manufacture</p>	<p>As per Tender Specification Article no 20</p>	
<p>General Features</p>	<p>a.The automatic fire suppression system design shall be strictly as per NFPA standard.</p> <p>b.It should be a Clean Agent Gas Based Automatic Fire Suppression System.</p> <p>c.The Seamless storage cylinder shall be for fire suppression system.</p> <p>d.The Valve operating actuators shall be of Electric (Solenoid) type. The actuators should be capable of being functionally tested for periodic servicing requirements.</p> <p>e.The individual cylinder bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure. This mechanism should be integrated as part of the actuator.</p> <p>f.The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.</p> <p>g.The detection and control system that shall be used to trigger the suppression shall employ cross zoning of smoke detectors. A single detector in one zone activated, shall cause an alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.</p> <p>h.The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc.</p> <p>i.The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's patented and certified software.</p> <p>j.Manual Gas Discharge stations and</p> <p>k.Manual Abort Stations shall be provided</p> <p>l.Manual Gas Discharge stations and</p>	

RESTRICTED

	Bidder will propose solution as per drawing & requirement.	
Refill	The system should be easily refillable	
Refill Support	The proposed Gas should be refillable up to year 2035.	
	Proper document should be provided to support the time line 2035.	
Interface	The system should be interfaced with the proposed building management system	
Software & Hardware	To integrate the system with the building management system if any software or/and hardware required it should be added.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

23. Access Control with visitor management System (Combination of IRIS (1unit), RFID & Biometric (1 unit) including 2 unit Exit Reader)]

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell or Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20 and South Korea	
Country of Manufacture	As per Tender Specification Article no 20	
	All the active components quoted for Access control system must be from a single OEM	
ACCESS CONTROLLER & Components	ACCESS DOORCONTROLLER UP TO 4 WIEGAND reader support	

RESTRICTED

	The access controller must be a rail mountable device for use in specific enclosures as well as existing standard 19" racks	
	The controller shall have a modular design with downloadable software so that the application program can be easily updated without touching the controller itself	
	Latest integrated 32-bit, 30 Mhz Micro-controller based system architecture;	
	On board Real Time Clock that will adjust itself to leap year computations automatically	
	ACCESS DOORCONTROLLER shall have 8 Relay outputs; 8 Analog Inputs; onboard LCD display 16 Characters	
	16-characters liquid crystal display (LCD), shall display network parameters and actual status like:	
	a. IP address of the controller	
	b. MAC address of the controller	
	c. DHCP on/off	
	d. Status of all the inputs connected to it	
	e. Status of all the outputs connected to it	
	f. Online and Offline status of the controller	
	g. Firmware version	
	ACCESS DOORCONTROLLER shall include a standard 2GB Compact flash (CF) memory card for storing cardholder data and access events.	
	Memory shall store database that has a capacity with a minimum of 80,000 cardholders and Event buffer size: maximum of 4,00,000 events with date and time stamp.	
	The access controller is UL 294, CE approved.	
	ACCESS DOORCONTROLLER housing shall be in accordance with UL 294 approved and is used for securely mounting and housing the Access Controller, extensions and the power supplies	

RESTRICTED

	<p>Power supply with battery charger for ACCESS DOORCONTROLLER Shall be with Selectable 12 VDC or 24 VDC voltage output Overvoltage protection Regulates battery charging voltage The product is classified in accordance with the following standards:</p> <ul style="list-style-type: none"> • EN 55022 Class B • EN 55024 • IEC / UL / EN 60950 & CSA (product safety) • CE <p>The Power supply can be mounted on rails and installed in the housing</p>	
Biometric Smart Card Reader	<p>The Finger-print biometric reader provided shall be of ruggedized design, having weatherized polycarbonate enclosure or similar protection to withstand harsh environments for both indoor/outdoor used and provides a high degree of vandal resistance with surface mounting style 13.56 MHz Biometric smart card Reader readers as per tender specifications</p>	
	<p>Biometric readers shall have CPU: ARM® Cortex™-A9 core 1GHz Biometric reader shall be with FBI PIV IQS certified optical fingerprint sensor Operating conditions: Temperature: -20°C to 55°C (-4°F to 131°F) – Humidity: 10% to 80% (non condensing) Ingress protection: IP65 Shall have 500 user capacity with expansion capacity of upto 10,000 users Accuracy shall be maintained regardless of number of users in database Biometric reader shall be with 2.8" QVGA color touchscreen and buzzer The specifier shall supply and install the necessary software to manage the Finger-print enrollment for all users and configuration of the Finger-print access control operations. The software provided shall be integrated to the Access Control System for access control and monitoring.</p>	
Smart Card Reader	<p>The Contact less Smart card reader shall provide authentication by reading the Card ID & controller will compare with database and</p>	

RESTRICTED

	<p>actuating the barrier/turnstile.</p> <p>Contactless smart card readers shall comply with ISO 15693 and shall read credentials that comply with these standards</p> <p>It shall be plug & Play type with suitable locking devices.</p> <p>It shall operate on its own. No software control is required for configuring the threshold sensitivity for readers</p> <p>It shall be possible to exchange the smart card reader without needing to reprogram the control unit</p> <p>The fault of /at one smart card reader shall not affect the functioning of other smart card readers on the network.</p> <p>The readers shall be powered by field panels itself. No external power supply should be used for powering the reader</p> <p>The Card reader shall conform to ISO 14443</p> <p>The Card reader shall be capable of reading the selected card technologies. (HID iClass/MiFareDESFire EV1 within the 14.56 MHz range).</p> <p>Shall use 64-bit authentication keys to reduce the risk of compromised data or duplicate cards. The contactless smart card reader and cards shall require matching keys in order to function together. All RF data transmission between the card and the reader shall be encrypted, using a secure algorithm.</p> <p>It shall have a read range of 5 cm – 7.5 cm when used with the accepted compatible access card technology</p> <p>It shall be capable of providing a unique tone and/or tone sequences for various status conditions such as access granted, access denied, reader power up, etc., and clear visual status LED indication (multi color) shall be provided for various status conditions.</p>	
	<p>Enhanced & optimized multi-tag inventory algorithm with the reading speed of more than 100 tags per second.</p> <p>Built-in 9dBi circular polarized antenna to read an RFID tag in any orientation from vehicle's windshield</p> <p>Supports INDIA 865~867 MHz, EU 865~868MHz, US 902~928MHz working</p>	

	<p>frequency</p> <p>Reliable read distance of up to 12 meters with IDCUBE's specialized ASSA series of long-range credentials</p> <p>Support EPC Global UHF class 1 gen2 / ISO18000-6C protocol RFID tags</p> <p>Integrates with Wiegand/RS232 compatible controllers</p> <p>Support for command, polling and trigger mode</p>	
Smart Cards	iCLASS Seos Contactless Smart Card, 8K memory	
	AES-128/2TDEA cryptographic algorithms for data protection Mutual authentication protocol with generation of diversified session key to protect each card session (using secure messaging)	
	Supports ISO/IEC standards: 7810, 7816 and contactless cards (14443 A)	
	Operating Temperature: - -40 to 70 degrees C and Operating Humidity 5% to 95% relative humidity non-condensing	
Access Control Software	<p>The Access Control System shall have a multi-level priority interrupt structure proven in multi-tasking and multi-client real time applications. Simultaneous alarms/events monitoring by multiple users, system supervision and history archiving shall be possible without degradation of any functionality specified for system or operation.</p>	
	The Access Control System server shall act as the source that provides time synchronization across all sub-systems.	
	<p>The Access Control System shall be capable to support to the following with additional expansion licenses if required:</p> <ul style="list-style-type: none"> • Number of active cardholders – 400,000 • Number of readers – 10,000 • Number of access groups – 255 • Number of time schedules – 255 • 4 – 8 digits programmable (Personal Identification Number) PIN codes • Remote Online Locks – 1,000 • Map viewer floor plans – 1,000 	

RESTRICTED

	<p>Operating Environment: The system server shall be use latest edition of Windows Server 2016 / 2019 and Client shall support Windows 10 shall include network capability with the TCP/IP data communications network protocol and hardware</p>	
	<p>Graphical User Interface: The system shall be a flexible and user-friendly workstation providing user(s) with a Graphical User Interfaces (GUIs) for alarm monitoring and control that includes map viewer with alarm list and a swipe ticker for visual door monitoring. The Access Control System GUI shall support single or multi screen displays having multiple dialogs separately. In case of alarms, the map will automatically focus on the alarm location.</p>	
	<p>Map Viewer and device overview: The system shall contain a map viewer. This map viewer shall provide a graphical presentation of the premises by means of floor plans, pictures or any desired graphical representation. On the maps entrances and devices like MAC, AMC, readers and digital input/outputs can be positioned as a dynamic icons. These graphical icons will display the location of the device in the map and the actual status of the device. Every icon can be displayed in several sizes, angle and color and background color. Clicking any of the devices automatically shows the commands available for controlling the respective device. Control commands are automatically linked based on device type. An operator can be assigned one or multiple authorizations for parts of the map viewer, such as door commands, reader commands, controller commands, system commands, special door commands, digital output commands, alarm list commands, swipe ticker commands. An area overview shall be able to show name, type (e.g. parking), current count, maximum count and state (e.g. empty, full). The ACS System must provide a real-time device overview of the entire system's status. All connected devices are shown on a status</p>	

RESTRICTED

	<p>tree. A direct control into subsystems is possible by clicking on panel/detector address. A device tree and the device names shall be provided for in the GUI.</p>	
	<p>Import Export tool: The Access Control System AS shall provide a web based import and export interface to import cardholder master records from a separate database during installation, or to export the master records for further use by another application in CSV format.</p>	
	<p>Areas The Access Control System shall provide the ability to define and manage arbitrary logical areas within the premises. These could be single rooms, groups of rooms, entire floors or parking areas.</p>	
	<p>Access Sequence Check There shall be an access sequence check provided, allowing authorized cardholders to enter an area only when they have swiped their card at the neighboring area.</p>	
	<p>Threat Level Management: At least 15 different threat levels can be pre-configured for instant activation in case of emergency. A threat level is activated by a threat alert. A threat alert can be triggered in one of the following ways:</p> <ul style="list-style-type: none"> • By a command in the software user interface • By an input signal defined on a local access controller, for instance from a push button or a fire panel. • By swiping an Alert card at a reader <p>Threat alerts can be cancelled by the UI command or hardware signal, but not by alert card.</p>	
	<p>Swipe Ticker: An application can be configured within the Map view that displays the last 10 minutes of access events in a dynamic scrolling list. The operator can easily pause and resume the display. Each record in the list contains details of the event and the credential used, for example:</p>	

RESTRICTED

	<ul style="list-style-type: none"> • The name of the cardholder and their stored photo, for visual confirmation of identity. • A time stamp. • Company and/or department name • The entrance and the reader at which the credential was used • An event category: Green- Access event Yellow- Incomplete access Red- Invalid access 	
	<p>Random screening: The Access Control System shall be able to perform an additional security check by the officer on duty. The readers are easily set to random screening mode by checking a checkbox and setting the frequency. If the randomizer selects this cardholder for extra security checks. The card is blocked throughout the whole system, until the block is manually removed. Once the screening is done, security can unblock the card or card can be unblocked after certain pre configured time.</p>	
	<p>Blocking cards: The Access Control System shall allow the blocking of cardholders as configured in the system, for example a defined validity period.</p>	
	<p>Alarm Handling and Management: The Access Control System AS shall provide a wide range of standard events. The following events, but not limited to, shall be supported:</p> <ul style="list-style-type: none"> • Card unknown • Card not authorized • Card outside time profile • Card anti-passback • Access timeout • Door open time exceeded • Door opened unauthorized • Door blocked • Tamper alarm controller • Tamper alarm reader • PIN code error • Duress alarm code • Access denied • Wrong card version • Card blocked 	

	<ul style="list-style-type: none"> • Card blacklisted • Card out route • Guard tour alarms • Random screening • Other individual alarm extensions <p>The Access Control System shall provide a wide range of standard events. All events are pre-configured in 4 alarm groups “hold-up”, “alarm”, “warning”, “maintenance”. The incoming alarm or event message shall provide, but not limited to, the following information:</p> <ul style="list-style-type: none"> •Alarm date and time •Alarm status •Alarm location <p>The Access Control System shall provide the operator a simple and efficient way to handle any incoming alarms. The operator shall be allowed to switch between all alarms or events messages. The Access Control System operator shall also be able to send remote commands or activate controls manually from the workstation when requested.</p>	
Accessories	Should be mention and quoted as per requirement	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

24. CCTV Surveillance System

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Bosch/Honeywell	

RESTRICTED

	or Equivalent)	
Model No.	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
	All the active components quoted for Access control system must be from a single OEM	
Physical Dimension	Please Mention	
NDA compliant	Should be NDA Compliant	
Resolution	Minimum 5 MP	
Image sensor type	Should have 1/2.7"	
Max. frames per second (fps)	Minimum 30@5MP	
Indoor / outdoor	Outdoor	
Quantity	a). Bullet IP Camera-10Nos b). PTZ IP Camera-2Nos c). Dome IP Camera-4Nos	
Built-in IR lighting	Should have 30 Meter / 98 Feet	
Wide Dynamic Range	Should have 120db	
ONVIF conformant	Should be ONVIF Conformant	
Power over Ethernet (PoE / PoE+)	Should have PoE Port	
Advanced Features		
Compression	Should have H.265, H.264, MJPEG	
Multi-streaming	Should have 3 streams	
Intelligent Dynamic Noise Reduction	Should have Intelligent Dynamic Noise Reduction	

RESTRICTED

Intelligent streaming	Should have Intelligent streaming	
Alarm triggering		
Video Analytics - pre-installed	Should ve IVA Pro Buildings	
Tamper detection	Should have temper detection	
Sensitivity		
Min. illumination day mode (color)	Should be 0.14 lux	
Min. Illumination night mode (B/W)	Should be 0 lux	
Lens		
Varifocal	Should be varifocal	
Automatic Varifocal (AVF)	Should be Automatic Varifocal (AVF)	
Iris control	Should have DC-iris	
Focal length from	Minimum 3.3 mm / 1.30 Inch	
Focal length till	Minimum 10.2 mm / 4.02 Inch	
Horizontal Angle of View (HAoV)	Minimum 30.1° x 101.4°	
Min. view angle (H)	Minimum 30.1°	
Min. view angle (V)	Minimum 21.8°	
Max. view angle (H)	Minimum 101.4°	
Max. view angle (V)	Minimum 69.6°	
Tilt angle	Minimum 0~85	
DCRI distances (in m with 100 lux illumination)		
Detection	Minimum 42m-193m	
Classification	Minimum 17m-77m	
Recognition	Minimum 9m-39m	

RESTRICTED

Identification	Minimum 4m-19m	
Storage		
(micro)SD-card slot	Should have (micro)SD-card slot	
Capacity of SD Card	Should have 64GB micro SD card in each camera from day one.	
Direct-to-iSCSI	Should able to connect with direct-to-iSCSI	
Housing		
Weather rating	IP66	
Vandal resistant	IK10	
Operating temperature	-30C to 50C (-22F to 122F)	
Network Video Recorder	Quantity-01	
Number of Channel	32	
Size of HDD	8TB or Higher surveillance / NAS grade hard disk.	
HDD slots	Minimum 4 slots, 3.5 in. SATA storage trays	
RAID support	Should support RAID-0,1,5 / 6	
Network	Should have dual Gigabit LAN (teamed)	
65" LED Display for CCTV view.	2Nos	
Power Consumption	Please mention	
Power Input	Please mention	
Form Factor	Should be rack mountable. Please mention	
USB Ports	Mim2	
Dimensions (H x W x D)	Please mention	
Weight	Please mention	
Operating Temperature	Please mention	
Non-operating	Please mention	

RESTRICTED

Temperature		
Operating Relative Humidity	Please mention	
Non-operating Relative Humidity	Please mention	

25. Raised Floor (Quantity: Approx 800SFT Set)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Arctiv/ RHGx600/ Maro or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Total Floor Area	Approx. 800sft. (Bidder will proposed as per drawing & requirement)	
Features of Solid Panel	1.Fiber-reinforced Calcium Sulphate Panel	
	2.Panel thickness: 32 mm minimum	
	3.High pressure laminate: 1.0mm HPL minimum	
	4.Uniform Load: 23000N/m ²	
	5.Point Load/Concentrated load: 450KG	
	6.Rolling Load: 4450N/10 times	
	7.Panel Weight: 18 KG approx	
	8.Concentrated Load: 450 KG	
	9.The panel shall meet the high requirements regarding dimensional accuracy acc. to RAL-GZ 941/EN12825 to guarantee high air tightness. High air leakage rate requirements are guaranteed as well.	

RESTRICTED

	10. Panel should be fire proof, dustproof and corrosion resistant	
	11. Panel size: 600 x 600 mm	
	12. Accessories: Pedestal, stringer, gasket etc.	
	13. Raised floor panels/tiles must be Anti-static with 1.5 Ft. high steel understructure.	
	14. The legs of the raised floor are all separate from each other	
	15. All legs of the raised floor are connected with earthing cable.	
	16. To pass the electric cable from the rack to the power socket under the raised floor proper cap to be used in the raised floor tiles.	
	17. The raised floor should be installed in such a way that the PAC for down flow and the proposed water detection system can be installed properly and can be serviced easily afterward.	
Features of Perforated Panel	1. Perforated steel panels designed for static load shall be interchangeable with standard field panels and capable of supporting concentrated loads with at least the load carrying capacity as the standard panels.	
	2. Panels shall have 58% or higher free air flow with Damper	
	3. Panel shall have damper added to control the airflow (optional)	
	4. The panel carrier plate consisting of a welded tube frame and must be conductive powder coated	
	5. Panel should made of non combustible materials	
	6. Panel size: 600 x 600 mm	
	7. Panel thickness: 32 mm minimum	
	8. Concentrate load: 3650N	
	9. Load bearing capacity: 16,100 N/m ²	

RESTRICTED

	10.Accessories: Pedistal, stringer, gasket etc.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

26. Data Center Floor insulation (Quantity: Approx 800SFT)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
Total Floor area	Approx. 800sft. (Bidder will proposed as per drawing & requirement)	
Features	<ul style="list-style-type: none"> g. A closed- cell structure not prone to wicking h. Mould resistance i. Dust and fiber-free construction j. An in- built water vapour barrier k. Ease of cutting and fitting l. Durability and maintenance 	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

27. Dry wall & Paint Works (Quantity: 1 Set)		
Feature List	Feature Description	Bidder Response
Dry wall	Fire rated two layer Gypsum Board Partition	
	10" Thickness two layer Gypsum board partition work with first class fire rated gypsum board. Inside the board should use glass wool to protect fire. MS Metal frame with all necessary accessories.	
Total area	Bidder will proposed as per drawing & requirement	
Paint work	Epoxy paint for inside server room, power room wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: To be mentioned	
	Country of manufacture: To be mentioned	
	Approved colour of epoxy paint to wall/column of inside wall,of the server room, power room, etc of two coats over a coat of brand specified primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding by roller/ spray etc and printing with two coats of epoxy paint approved color over a coat of priming etc all complete as per direction	
	Normal Paint for noc room and other wall and ceiling	
	Brand: To be mentioned	
	Country of Origin: Bangladesh	
	Country of manufacture: Bangladesh	
	approved colour of normal paint to wall/column of inside wall,of the NOC, staging, open area etc of two coats over a coat of brand specified	

	primer / scalar collapsing specified time for drying/recoating including cleaning, drying, making free from dirt grease, wax, removing all chalked and scald materialism fungus, mending grid the surface defects, sand papering the surface and necessary scaffolding by roller/spray etc and printing with two coats of normal paint approved color over a coat of priming etc all complete as per direction	
--	--	--

27. Water Leak Detection System to cover Data Center floor (Server & Power rooms) all critical areas & points) embedded with Monitoring & Notification

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of Manufacture	As per Tender Specification Article no 20	
General requirement	Water Leak Detection System to cover Data Center floor (Server & Power rooms) all critical areas & points) embedded with Monitoring & Notification	
Floor area to be covered	Bidder will propose as per design & requirement.	
Features	<ul style="list-style-type: none"> i. should be able to detect the moisture bellow the raised floor. m. It should provide immediate warning after detecting the moisture and water. n. It should be Micro-Processor Based Control 	

RESTRICTED

	<ul style="list-style-type: none"> o. Monitors each zone independently. p. Provides subsequent alarming, no matter how many zones go into ALARM or FAULT. q. Identifies location, time & date of all ALARM and FAULT conditions. r. Alarming should be provided at-least via two or more of the below state method Audible Visual s. In-band and out-of-band methods indicating in the software console and/or in the Building management system. t. Monitoring software should be provided with the system. u. Each cable length should be 20 feet or higher. v. To provide the solution if any other component has to add it should be included and the price should be required. 	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years full warranty	

29. Lightning Protection System		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of manufacturer	As per Tender Specification Article no 20	
General Features	d. A lightning protection system includes a network of air terminals, bonding conductors, and ground electrodes designed to provide a low impedance path to ground for potential strikes.	

RESTRICTED

	e. Required resistance <1 Ohm f. Grounding rods, inspection pit, lightning event counter have to be considered.	
--	--	--

30. Rodent System		
Brand	To be mentioned (Preferably Maser or Equivalent)	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Master controller	Bidder will offer advanced rodent repellent system considering as per drawing.	
Transducer	Bidder will offer transducer considering as per drawing.	
Wire bundle	Wire bundle	
Installation	Installation Material, Testing & Commissioning Charge	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

31. Fire rated door for data center (double leaf (5'0"X7'))		
Brand	To be mentioned	
Origin	To be mentioned	
Country of Origin	As per Tender Specification Article no 20	
Country of Manufacturer	As per Tender Specification Article no 20	
Feature		
Fire rating	for 120 Minutes, Conforms to IS3614 (PART-2)1992, BS476 (PART 20 & 22) and ISO834.	
Material:	Door Frames and Leaves are made from Galvanized Steel	

RESTRICTED

Door Leaves:	Constructed from 2.0mm thick galvanized steel sheet formed to provide a 48mm thick fully flush, double skin door shell with seamless welding joint all around. The internal construction of the door shall be specially designed with infill to give 2 hours fire rating.	
Infill:	All the doors will have Honey Comb Crafted Paper or equivalent infill.	
Vision panel:	Fire Rated glass vision panel	
Accessories	Hinge, bolt and screw: Fire rated Lock: Built in mortise lock Auto Door Closer: Default Push panic bar: built in	
Standards	UL Listed Fire door NFPA 251 Standard Test standard: Fire Door must be tested according to BS Standard	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Warranty	Three (03) years full warranty	

PASSIVE HARDWARE FOR UDC-Command HQ & UDC-BASE and Network

1. Server Rack with KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider/ / Vertiv / Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1500 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	Ø 04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	Ø 04 units 1U Universal Horizontal Cable Manager	
	Ø 04 units 2U Universal Horizontal Cable Manager	
Vertical Cable Manager	At least 4 Vertical cable managers should be provided with each rack.	
Fixed trays/shelves	2 Fixed trays/shelves capable of caring at least 50 kg load, depth of at least 900 mm should be provided with each rack	
Sliding trays/shelves	1 Sliding trays/shelves should be provided with each rack	

RESTRICTED

Tool less Airflow Management Blanking Panels	At least 20 U blank panel should be provided with each rack	
Stabilization	Should be provided	
Rack Monitor	17" TFT rack mount APC/Vertiv/Arctiv or equivalent monitor which occupies only 1 U / 2U rack space	
	1 unit for each rack	
Integrated Keyboard and Mouse	Required with sliding functionality	
Power Distribution Unit (PDU) with built-in K-type transformer	Switched Rack PDU, 32A – At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
	Metered Rack PDU, 32A – At least 42 way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
KVM Switch	Switch that allows 2 users (one remote & one local User) single-point access and control of up to 16 multiple servers from a single console with 16 units KVM console cable and 16 units 1.5mtr cat 6 & 16 units 3mtr cat 6 patch cord	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each Rack to connect the servers/network/PDU equipment with the quoted rack.	
	02 units of C20 to industrial female (32A)	
	02 units of C19 to industrial male (32A)	
	02 units of C14 to industrial female (16A)	
	02 units of C13 to industrial male (16A)	
	04 units of C19 to C20 cable (16A, 3m).	
	10 units of C13 to C14 cable (10A, 3m).	
	10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

2. Rack without KVM		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	42U EIA-310-D compliant Closed Rack	
Width	750mm to 800 mm	
Depth	At least 1200 mm depth	
Weight	Total Weight bearing capacity at least 1200 Kg	
Perforated door	All doors should be Perforated (Front & Rare)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	500 units Should be provided	
U Positions	Should be numbered	
Leveling Feet and Casters wheel	Should be Pre-installed and easily adjustable	
Cable access on the roof of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead cable troughs	
Rear Cabling Channels	Multi-purpose cable management	
	Tool less mounting for Rack PDUs	
	Tool less mounting of cable management accessories	
	Side access holes for cross- connecting between adjacent racks with sides removed	
Horizontal Cable Manager	04 units 1U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 2U Brush Strip Horizontal Rack Cable Management Panel with Brush Plate Network Cable Manager	
	04 units 1U Universal Horizontal Cable Manager	
	04 units 2U Universal Horizontal Cable Manager	
Tool less Airflow Management	At least 20 U blank panel should be provided with each rack	
Blanking Panels		
Stabilization	Should be provided	
Power Distribution Unit	Metered Rack PDU, 32A – At least 42	

RESTRICTED

(PDU) with built-in K-type transformer	way, 02 units:	
	Active monitoring and alarms to warn of potential overloads	
	Switched Rack PDU, 32A– At least 24 way, 02 units:	
	Remotely control and fully manage individual receptacles plus active monitoring and alarms to warn of potential overloads	
Software	Software should be provided to Monitor and control the Switched PDUs and Metered PDUs	
Cables	50 no. of Power cable should be provided with each ATS to connect the servers/network/PDU equipment with the quoted ATS.-	
	02 units of C20 to industrial Male (32A)	
	02 units of C19 to industrial Female (32A)	
	12 units of C19 to C20 cable (16A, 3m).	
	10 units of C19 to C20 cable (16A, 2m)	
	10 units of C13 to C14 cable (10A, 3m).	
	10 units of C13 to C14 cable (10A, 2m).	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

3. 9U wall mountable network rack for Building (Access Switch)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	9U or above EIA-310-D compliant Closed Rack	
Width	600mm to 700 mm	
Depth	600mm to 800 mm	
Weight	Total Weight bearing capacity at least 500 Kg	
Glass door	All doors should be glass (Front)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	50 units Should be provided	
U Positions	Should be numbered	

RESTRICTED

Cable access on the roof & bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead or bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 01 units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

4. 9U wall mountable network rack for Floor (Access Switch)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	9U or above EIA-310-D compliant Closed Rack	
Width	600mm to 700 mm	
Depth	600mm to 800 mm	
Weight	Total Weight bearing capacity at least 500 Kg	
Glass door	All doors should be glass (Front)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	50 units Should be provided	
U Positions	Should be numbered	
Cable access on the roof & bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead or bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 01 units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

5. 6KVA Online UPS for UDC Server room with 15 Minutes backup		
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity:	Minimum 6 KVA	
Output power factor:	Please mention	
Topology:	True online double conversion	
Input		
Voltage range:	110~280 Vac (Single + G)	
Frequency range:	45-70Hz (auto sensing)	
Input power factor:	≥ 0.99 @ 100% linear load	
Input Current Distortion:	$\leq 3\%$ (full load)	
Output		
Output voltage:	200/208/220/230/240 Vac (Single + G)	
Output voltage distortion:	$<1\%$ @ 100% Linear Load; $<3\%$ @ 100% Non-Linear Load	
Output voltage regulation:	$\pm 1\%$	
Frequency range:	$\pm 1\text{Hz}$ or $\pm 3\text{Hz}$ (selectable)	
Output waveform:	Pure sine wave	
Overload Capacity Inverter:	$<105\%$ continuous 105-125% for 600 to 30 seconds	
	transfer to bypass. 125-150% for 30 seconds to immediately transfer to bypass.	
EFFICIENCY:	90% or higher	
ENVIRONMENTAL:	Operation Temperature 0~40°C / 32~104°F	

RESTRICTED

Operation Humidity:	20~95%RH (without condensing)	
Altitude:	1000m/3280ft without derating"	
STANDARDS AND CERTIFICATIONS:	Safety: IEC / EN62040-1, UL1778; EMC: EN62040-2, EN61000-3-2, EN61000-3-3	
FCC Class A Performance:	IEC / EN62040-3	
Manufacturing:	ISO 9001:2015, ISO 14001:2015 / CE, UL, cUL, FCC	
Battery Capacity:	To be mentioned in Ah	
Brand:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	To be mentioned	
Model:	To be mentioned	
Weight of Battery (Kg):	Please mention	
Battery Cabinet:	<ul style="list-style-type: none"> a. Battery cabinet should be from the same OEM make. b. The Cabinet architecture should be load distributed and Compact height type. c. The Cabinet structure should be made with heavy load carrying material. d. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. e. The cabinet color should be best quality powder coated. f. A Circuit breaker metal box should be install in the cabinet for isolating the battery. g. The breaker box should have an easy-to-open option. h. The Circuit Breaker Capacity should be as per OEM recommendation. i. Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	

RESTRICTED

Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	
-----------	---	--

6. AC Controller		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Function	Timer based controller for controlling two split AC.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

7. Split AC (min 2.0 ton) for Room Size 200 SFT		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Daikin/DahmBosh /General or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity :	2.0 ton.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

8. Split AC (1.5 ton)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Daikin/DahmBosh /General or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	

RESTRICTED

Country of manufacturer	As per tender specification article 20	
Capacity :	1.5 ton.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

9. Access Control Reader (Stand Alone)

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of Origin	As per tender specification article 20 and South Korea	
Country of manufacturer	As per tender specification article 20	
Feature	01 x Stand Alone Biometric Reader & 1X Exit reader with 05 x Access Card to be provided for each UDC.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

10. CCTV System for UDC

Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
3X 4 MP IP Bullet Camera	<p>Image Sensor: 1/3"- 1/2.7" progressive scan super low lux CMOS or better</p> <p>IR Distance: Minimum 30 mtr (98.4 ft)</p> <p>Lens: Varifocal lenses with remote zoom and focus</p> <p>Night Vision: IR illumination with a range of at least 30 meter & Low-light performance (minimum 0.01 lux)</p> <p>Housing: IP67</p>	

RESTRICTED

	Features: Wide Dynamic Range (WDR) of 120dB or higher, Motion detection, Intrusion detection, Tamper detection, Audio recording (optional, subject to local regulations), Smart analytics (face recognition, people counting, object removal detection)	
1X Network Video Recorder (NVR)	<ol style="list-style-type: none"> 1. NVR should have at least 8 Channel 2. Should have 8 or higher PoE RJ45 port. 3. Minimum 2 number of surveillance/NAS type hard disk should be installed. 4. Decoding format: H.265/H.264/H.264/H.265+ 5. Supported Resolution 4MP, 1080p, 720p, 4CIF, 2CIF, CIF 6. Storage rate: 30 fps or more 7. HDD Interface: 2 Bay or more 8. Video Recording Res: Upto 8 MP 9. Capacity: Minimum 4 TB capacity for each bay 10. Software Management: ONVIF supports different platform software 	
1X LED 50" Monitor	<p>Brand: To be mentioned</p> <p>Model: To be mentioned</p> <p>Country of origin: As per tender specification, article 20</p> <p>Manufacturing Country: As per tender specification, article 20</p>	
1 X 17" LED monitor	<p>Brand: To be mentioned</p> <p>Model: To be mentioned</p> <p>Country of origin: As per tender specification, article 20</p> <p>Manufacturing Country: As per tender specification, article 20</p>	
2X HDD 4TB	<p>Brand: To be mentioned</p> <p>Model: To be mentioned</p> <p>Country of origin: As per tender specification, article 20</p> <p>Manufacturing Country: As per tender</p>	

RESTRICTED

	specification, article 20	
Other Accessories	Others items required to make the full system operational are to be provided by the bidder	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

11. CCTV System for 400 Access Switch location in 28 UDC		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
2X 2 MP IP Bullet Camera for 400 access switch location.(Total 800 nos).		
Feature of 2MP IP camera.	<p>Image Sensor: 1/3"- 1/2.7" progressive scan super low lux CMOS or better</p> <p>IR Distance: Minimum 30 mtr (98.4 ft)</p> <p>Lens: Varifocal lenses with remote zoom and focus</p> <p>Night Vision: IR illumination with a range of at least 30 meter & Low-light performance (minimum 0.01 lux)</p> <p>Housing: IP67</p> <p>Features: Wide Dynamic Range (WDR) of 120dB or higher, Motion detection , Intrusion detection, Tamper detection, Audio recording (optional, subject to local regulations) , Smart analytics (face recognition, people counting, object removal detection)</p>	
28 X Network Video Recorder (NVR) server in 28 UDC location		
Processor	Minimum Intel Xeon Processor E3-1275 V3 (8 MB Cache, 3.5 GHz) processor	
Cache	Minimum 8 MB Intel Smart Cache	
Memory	Minimum 8 GB, DDR3-1666 ECC UNB (1 x 8 GB)	
HDD slots	Minimum 8 slots, 3.5 in. SATA storage trays	

RESTRICTED

HDD for video	Minimum 8TB/HDD Total Number of HDD 8Nos.	
SSD for OS	Minimum 2 x 120 GB SSD drives in RAID-1 configuration	
OS	Should have Windows Storage Server 2012 R2 license built in	
RAID support	Should support RAID-5 / 6	
Protocol	Should be iSCSI	
B/W capacity	Minimum 550 Mbit/s	
Network	Should have dual Gigabit LAN (teamed)	
Hot swappable HDDs	Yes	
Hot swappable power supply, fans	Yes	
Form Factor	Should be rack mountable. Please mention	
USB Ports	Should have Front: 2 USB 2.0 ports, Rear: 2 USB 2.0 ports, 2 USB 3.0 ports	
Dimensions (H x W x D)	Please mention	
Weight	Please mention	
Operating Temperature	Please mention	
Non-operating Temperature	Please mention	
Operating Relative Humidity	Please mention	
Non-operating Relative Humidity	Please mention	
Quality	This product shall be manufactured by a firm whose quality system is in compliance with the I.S. /ISO 9001/EN 29001, QUALITY SYSTEM.	
SNMP	Should support Simple Network Management Protocol is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.	
1X LED 55" Monitor	Brand: To be mentioned	

RESTRICTED

	Model: To be mentioned Country of origin: As per tender specification, article 20 Manufacturing Country: As per tender specification, article 20	
1 X 17" LED monitor	Brand: To be mentioned Model: To be mentioned Country of origin: As per tender specification, article 20 Manufacturing Country: As per tender specification, article 20	
Other Accessories	Others items required to make the full system operational are to be provided by the bidder	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

12. 3KVA Online UPS for different UDC's building with 15 Minutes backup

Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity:	Minimum 3 KVA	
Output power factor:	Please mention	
Topology:	True online double conversion	
Input		
Voltage range:	110~280 Vac (Single + G)	
Frequency range:	45-70Hz (auto sensing)	
Input power	≥ 0.99 @ 100% linear load	

RESTRICTED

factor:		
Input Current Distortion:	≤ 3% (full load)	
Output		
Output voltage:	200/208/220/230/240 Vac (Single + G)	
Output voltage distortion:	<1%@100% Linear Load; <3% @100% Non-Linear Load	
Output voltage regulation:	±1%	
Frequency range:	±1Hz or ±3Hz (selectable)	
Output waveform:	Pure sine wave	
Overload Capacity Inverter:	<105%continuous 105-125% for 600 to 30 seconds	
	transfer to bypass. 125-150% for 30 seconds to immediately transfer to bypass.	
EFFICIENCY:	90% or higher	
ENVIRONMENTAL:	Operation Temperature 0~40°C / 32~104°F	
Operation Humidity:	20~95%RH (without condensing)	
Altitude:	1000m/3280ft without derating"	
STANDARDS AND CERTIFICATIONS:	Safety: IEC / EN62040-1, UL1778; EMC: EN62040-2, EN61000-3-2, EN61000-3-3	
FCC Class A Performance:	IEC / EN62040-3	
Manufacturing:	ISO 9001:2015, ISO 14001:2015 / CE, UL, cUL, FCC	
Battery Capacity:	To be mentioned in Ah	
Brand:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of Manufacture:	To be mentioned	
Model:	To be mentioned	
Weight of Battery	Please mention	

RESTRICTED

(Kg):		
Battery Cabinet:	<ul style="list-style-type: none"> a. Battery cabinet should be from the same OEM make. b. The Cabinet architecture should be load distributed and Compact height type. c. The Cabinet structure should be made with heavy load carrying material. d. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. e. The cabinet color should be best quality powder coated. f. A Circuit breaker metal box should be install in the cabinet for isolating the battery. g. The breaker box should have an easy-to-open option. h. The Circuit Breaker Capacity should be as per OEM recommendation. i. Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

13. 1KVA Online UPS for UDC's different floor with 15 Minutes backup		
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity:	Minimum 1 KVA	
Output power factor:	Please mention	
Topology:	True online double conversion	
Input		

RESTRICTED

Voltage range:	110~280 Vac (Single + G)	
Frequency range:	45-70Hz (auto sensing)	
Input power factor:	≥ 0.99 @ 100% linear load	
Input Current Distortion:	≤ 3% (full load)	
Output		
Output voltage:	200/208/220/230/240 Vac (Single + G)	
Output voltage distortion:	<1%@100% Linear Load; <3% @100% Non-Linear Load	
Output voltage regulation:	±1%	
Frequency range:	±1Hz or ±3Hz (selectable)	
Output waveform:	Pure sine wave	
Overload Capacity Inverter:	<105%continuous 105-125% for 600 to 30 seconds	
	transfer to bypass. 125-150% for 30 seconds to immediately transfer to bypass.	
EFFICIENCY:	90% or higher	
ENVIRONMENTAL:	Operation Temperature 0~40°C / 32~104°F	
Operation Humidity:	20~95%RH (without condensing)	
Altitude:	1000m/3280ft without derating"	
STANDARDS AND CERTIFICATIONS:	Safety: IEC / EN62040-1, UL1778; EMC: EN62040-2, EN61000-3-2, EN61000-3-3	
FCC Class A Performance:	IEC / EN62040-3	
Manufacturing:	ISO 9001:2015, ISO 14001:2015 / CE, UL, cUL, FCC	
Battery Capacity:	To be mentioned in Ah	
Brand:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of	To be mentioned	

RESTRICTED

Manufacture:		
Model:	To be mentioned	
Weight of Battery (Kg):	Please mention	
Battery Cabinet:	<ul style="list-style-type: none"> a. Battery cabinet should be from the same OEM make. b. The Cabinet architecture should be load distributed and Compact height type. c. The Cabinet structure should be made with heavy load carrying material. d. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. e. The cabinet color should be best quality powder coated. f. A Circuit breaker metal box should be install in the cabinet for isolating the battery. g. The breaker box should have an easy-to-open option. h. The Circuit Breaker Capacity should be as per OEM recommendation. i. Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

PASSIVE HARDWARE FOR UDC-SHIP and Network

1. 25U Floor Stand and wall mountable network rack for Ship		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	25U or above EIA-310-D compliant Closed Rack	
Width	600mm to 700 mm	
Depth	1000mm or higher	
Weight	Total Weight bearing capacity at least 1000 Kg	
Perforated door	All doors should be perforated (Front)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	100 units Should be provided	
U Positions	Should be numbered	
Cable access on the roof & bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead or bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 02 units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

2. 15U Floor Stand and wall mountable network rack for Ship		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	15U or above EIA-310-D compliant Closed Rack	
Width	600mm to 700 mm	
Depth	1000mm or higher	
Weight	Total Weight bearing capacity at least 1000 Kg	

RESTRICTED

Perforated door	All doors should be perforated (Front)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	100 units Should be provided	
U Positions	Should be numbered	
Cable access on the roof & bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead or bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 02 units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

3. 6U wall mountable network rack for Ships

Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	6U or above EIA-310-D compliant Closed Rack	
Width	600mm to 700 mm	
Depth	600mm to 800 mm	
Weight	Total Weight bearing capacity at least 500 Kg	
Glass door	All doors should be glass (Front)	
	All door should have locks	
Extension bars	Should be provided as required	
Cage nuts & screws	50 units Should be provided	
U Positions	Should be numbered	
Cable access on the roof & bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for overhead or bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 01 units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

4. Access Control Reader (Stand Alone)		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned	
Model	To be mentioned	
Country of Origin	To be mentioned	
Country of manufacturer	To be mentioned	
Feature	01 x Stand Alone Biometric Reader & 1X Exit reader with 05 x Access Card to be provided for each UDC.	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

5. 1KVA Online UPS, rack mountable in 6U or above rack with 600mm depth rack for Ships with 15 Minutes backup		
Brand	To be mentioned (Preferably Schneider / Vertiv/ Centiel / Equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification article 20	
Country of manufacturer	As per tender specification article 20	
Capacity:	Minimum 1 KVA	
Form factor	19" rack mountable	
Depth	Should not be more than 600mm	
U required	Please mention the number of U required	
Output power factor:	Please mention	
Topology:	True online double conversion	
Input		

RESTRICTED

Voltage range:	110~280 Vac (Single + G)	
Frequency range:	45-70Hz (auto sensing)	
Input power factor:	≥ 0.99 @ 100% linear load	
Input Current Distortion:	$\leq 3\%$ (full load)	
Output		
Output voltage:	200/208/220/230/240 Vac (Single + G)	
Output voltage distortion:	$<1\%$ @100% Linear Load; $<3\%$ @100% Non-Linear Load	
Output voltage regulation:	$\pm 1\%$	
Frequency range:	$\pm 1\text{Hz}$ or $\pm 3\text{Hz}$ (selectable)	
Output waveform:	Pure sine wave	
Overload Capacity Inverter:	$<105\%$ continuous 105-125% for 600 to 30 seconds	
	transfer to bypass. 125-150% for 30 seconds to immediately transfer to bypass.	
EFFICIENCY:	90% or higher	
ENVIRONMENTAL:	Operation Temperature 0~40°C / 32~104°F	
Operation Humidity:	20~95%RH (without condensing)	
Altitude:	1000m/3280ft without derating"	
STANDARDS AND CERTIFICATIONS:	Safety: IEC / EN62040-1, UL1778; EMC: EN62040-2, EN61000-3-2, EN61000-3-3	
FCC Class A Performance:	IEC / EN62040-3	
Manufacturing:	ISO 9001:2015, ISO 14001:2015 / CE, UL, cUL, FCC	
Battery Capacity:	To be mentioned in Ah	
Brand:	To be mentioned	
Country of Origin:	As per Tender Specification Article no 20	
Country of	To be mentioned	

RESTRICTED

Manufacture:		
Model:	To be mentioned	
Weight of Battery (Kg):	Please mention	
Battery Cabinet: (If required)	<ul style="list-style-type: none"> a. Battery cabinet should be from the same OEM make. b. 19" rack mountable c. Depth should not be more then 600mm. d. Please mention the number of U required e. The Cabinet architecture should be load distributed and Compact height type. f. The Cabinet structure should be made with heavy load carrying material. g. The Cabinet frame should be made by MS Box and battery bed should be made with MS U Channel. h. The cabinet color should be best quality powder coated. i. A Circuit breaker metal box should be install in the cabinet for isolating the battery. j. The breaker box should have an easy-to-open option. k. The Circuit Breaker Capacity should be as per OEM recommendation. l. Each and Every battery should be equipped with Battery lead cap, busbar for battery-to-battery connection, busbar insulator 	
Installation:	Supply, installation, testing, and commissioning by OEM-certified engineer.	
Warranty:	3 (three) years Full warranty with quarterly preventive maintenance and onsite support with parts, labor, replacement. 24/7 Support and respective team should be assigned on site within 2 (two) hours after reporting the incident from the bank.	

6. 12U Floor Stand outdoor type network rack for Ship Jetty		
Feature List	Feature Description	Bidder Response
Brand	To be mentioned (Preferably Schneider//Vertiv/Arctiv or equivalent)	
Model	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of manufacturer	As per tender specification, article 20	
Height	12U or above EIA-310-D compliant	

RESTRICTED

	Closed Rack	
Width	600mm to 700 mm	
Depth	600mm or higher	
IP rating	67IP rated	
Characteristic	<ol style="list-style-type: none"> 1. Should withstand harsh weather 2. Should be water proof 3. Should be corrosion proof 4. Should be able to weild with the jetty 	
Door	Door should be lock able	
Extension bars	Should be provided as required	
Cage nuts & screws	100 units Should be provided	
U Positions	Should be numbered	
Cable access on the bottom of the rack.	Multiple cable access slots	
	Multiple mounting holes for bottom cable troughs	
Power Distribution Unit (PDU) with built-in	Rack PDU, 16A – At least 8way UK point , 01units:	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	
Certificates	Machine must comply tier-3 compliance (Uptime Institute/epi) in all aspects	
Warranty	Three (03) years	

TENDER SPECIFICATION OF 800KVA SUB STATION CDC

Products Names/Items	Description of requirements	Bidder Response
1.EXPRESS LINE FEEDER with RMU & HT Metering panel		
General Requirements	For 2X800KVA substation the express line feeder from nearby RMU (or with RMU if required), HT Metering panel shall be required. Bidder will coordinate with local power supply authority and will plan and propose accordingly.	

2.11KV Isolator with vacuum contactor		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	Rated Current: 630 Amps Voltage Rating: 11kV (or as specified based on system requirements) Short-Circuit Rating: Ensure compatibility with system short-circuit requirements, typically around 25kA or as specified. Mounting: Indoor, Floor-mounted as per substation design. Type: 11KV Isolator with vacuum contactor Standards Compliance: Must comply with IEC 62271-102 for high-voltage switchgear and control gear isolators. Protection Class: IP54 or IP65, depending on environmental exposure and dust/moisture levels.	

3. HT AUTOMATIC VOLTAGE REGULATOR (AVR) WITH BYPASS ARRANGEMENT		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	a. The HT Automatic Voltage Regulator/Controller (HT AVR) shall be 11KV copper wound suitable for input voltage range from 8 KV to 12KV with output stabilized at 11 KV + 1%, indoor, oil-immersed, naturally cooled, on load, step	

RESTRICTED

	less type with rolling contacts.	
	b. The principle of operation of HT AVR shall be auto transformer, tapped continuously with the aid of rolling contact mechanism moved by self-powered FHP synchronous motor for stabilizing output voltage automatically.	
	c. Correction of voltage shall also be possible by motor through push buttons. If Automatic and motorized control become defunct, correction of voltage shall be possible by means of a hand wheel.	
Standards:	The HT AVR shall conform to the relevant BS/IS specification with upto date amendments	
Power supply parameters:	a. The HT AVR shall be capable of continuous operation as specified rating.	
	b. The HT AVR shall be designed to give stabilized output voltage at 11000 V + 1%, 3 Phase, 50 Hz, suitable for balanced input & unbalanced load, when the input voltage varies between 8000 V to 12000 V, 3 phase, 50 Hz. On 11 KV 3 phase, 50 Hz. System.	

4. 11 KV H.T. SWITCHGEAR (VCB)		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>11 KV H.T. SWITCHGEAR (630 A, VCB) Sheet steel clad 14 SWG, Powder Coated dust and vermin proof, freestanding, floor mounting indoor HT Switchgear 11KV, 50Hz, three phase, 800 A hard drawn electrolytic copper busbars equipped with:</p> <p>a) 1 No. 630 A, 11 KV, breaking current 25KA (3 sec.), making current 50 KA, 50 Hz, TP Vacuum Circuit Breaker (Fixed Type) with motor operated mechanism with closing solenoid shunt releases,</p>	

RESTRICTED

	<p>auxiliary contacts 5NO + 5NC and limit switch (1 'NO + 1 NC) for indication "Closing spring charged". mechanical on/off/trip indicator. Origin : To be mention by bidder</p> <p>b) 3 Nos. Cast resin insulated, double pole, Potential Transformer, ratio: $11\sqrt{3}/.11/\sqrt{3}$ KV, Class 0.5, 50 VA, Origin : To be mention by bidder</p> <p>c) 1 No. MCB of adequate rating for PT Secondary Protection.</p> <p>d) 3 Nos. Cast resin insulated, 11 KV dry type double 'core CT with Ratio: 60/5/5A, 1st core for metering, 2nd for protection Core 1 : 10 VA, Class 0.5M5 Core 2 : 15 VA, Class 10P10 Origin : To be mention by bidder.</p> <p>e) 3 Nos. Digital Ammeter, 0 - 60 A. 1 No. Digital Voltmeter, 0 - 15 KV, with selector switch 1 No. Triple pole IDMT Solid State type Relay for over current, Earthfault and short circuit protection, Control voltage - 110 V DC Origin : To be mention by bidder.</p> <p>f) 2 Nos. ON and OFF/TRIP Push Button 2 Nos. Indicating Lamps ON and OFF/TRIP 1 No. Panel Heater</p> <p>Any other changes at HT panel equipment/ component shall be considered for proper load management/distribution.</p>	
--	--	--

5. 800kVA CAST RESIN DRY TYPE TRANSFORMER		
Brand	To be mentioned (Preferably Schneider/Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	800kVA, 11/0.415kV Cast Resin Dry Type Transformer with Canopy Three phased cast resin dry transformers, class F1, E2,	

RESTRICTED

	<p>C2, indoor use, with standard accessories. Design manufacturing, routine tests & tolerances according to IEC 60076-11 standards. Standard fittings: 4 flat bi-directional rollers. 2 lifting lugs 2 earthing points. 1 rating plate(on HV side) HV/ LV connections: Connection from top onto flat bar terminals. Enclosure: IP31 Quality Assurance: Transformer shall be made according to system of quality assurance with (quality assurance in design, production and servicing) standards ISO 9001, certificate AFAQ bn 1993/1275</p>	
<p>Technical Data:</p>	<ol style="list-style-type: none"> 1. Rated power: 800KVA 2. Rated frequency: 50Hz 3. Rated lightning impulse withstand voltage BIL 1.2/ 50μs HV :75kV peak LV :8kV peak 4. Rated power frequency withstand voltage 50Hz 1mn HV :28kV rms LV :3kV rms 5. Rated insulation level HV :12kV LV :1.1kV 6. Rated voltage Primary :11kV Secondary at no load : 0.415kV 7. Tap changer links (in HV winding): Type Off load in tapping range : % +5 to -5 Per step size : 2.50% Step/ Position No. : 5-Apr 8. Vector group : Dyn11 9. Maximum ambient temperature : 40°C 10. Maximum installation altitude above sea level: 1000m 11. Cooling System : AN 12. Installation : Indoor 13. Winding Material : HV/ LV(As per industry standard) 14. Loss: No load loss : 1300W 	

RESTRICTED

	<p>Load loss at 75°C : 8000W 15. Rated impedance voltage at 75°C : 6% 16. Thermal class insulation : Class F 17. Temperature rise : 100K 18. Acoustic power LwA : 69dB (A) 19. Acoustic pressure LPA at 1.00m : 56dB (A) Raw Materials: A) Brand: To be mentioned. B) Model: To be mentioned. C)COO: To be mentioned. D) COM: To be mentioned.</p>	
<p>TESTS AT MANUFACTURER'S SITE</p>	<p>The following tests shall be performed at manufacturer's site prior to packing and dispatch.</p> <p>a.No Load loss b.No load excitation current c.Load losses and impedance voltage d.Dielectric tests e.Switching impulse test f.Lightning impulse test g.Partial discharge test h.Insulation power factor i.Noise measurement j.Temperature rise (Heat run) Short circuit test</p>	

6. Phase Correction Device (PCD)-1600A,		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20a	
Manufacturing Country	As per Tender Specification Article no 20a	
General Features	<p>a. 16 SWG sheet steel enclosed, type tested, dust and vermin proof, free standing floor stand indoor type, powder coated paint finished.</p> <p>b. The PCD busbar will be hard drawn electrolytic required Amp copper busbar, properly insulated.</p> <p>c. TPN & E equipped with insulator, internal cover for busbar section.</p> <p>d. Digital multimeter to show 3 phase's volts, amp, etc.; indicator lamp-3pcs per phase, phasing preventor relay 3 pcs for phase correction; AC electronic Relay 3 pcs, DC electronic</p>	

RESTRICTED

	<p>relay - 3 pcs, timer Second -6 pcs.</p> <p>e. During design bidder will consider appropriate bus bar, breaker, protection devices, monitoring devices for SCADA/DCIM monitoring.</p> <p>f. Fully automatic phase reversal correction. Load Protection from High or Low voltage.</p> <p>g. Selectable switch for high and low voltage selection.</p> <p>h. Nominal voltage will be minimum 400V. Nominal operating current will be 1600A or as required to construct the data center.</p>	
--	---	--

7. LT SWITCHGEAR 1600A, ACB with Bus bar Coupler & 2XMDB-1250A, ACB		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features of LT panel 1&2	<p>Incoming :</p> <p>a. 1 No. 1600 A, 70 KA, TP ACB with thermal overload and adjustable magnetic short-circuit releases</p> <p>b. 3 Nos. Current Transformer, ratio: 1600/5A with suitable accuracy and burden</p> <p>c. 3 Nos. Ammeter, 0 - 1600 A</p> <p>d. 1 No. Voltmeter, 0 - 500 V with selector switch</p> <p>e. 3 Nos. Phase Indicating Lamp</p> <p>Outgoing:</p> <p>2 No. 1250A,50 KA, TP ACB with thermal overload and adjustable magnetic short-circuit release.</p>	
	Any other changes at LT panel equipment/ component shall be considered for proper load management/distribution.	

RESTRICTED

<p>General Features of MDB 1&2</p>	<p>Incoming :</p> <ul style="list-style-type: none"> f. 2No. 1250 A, 70 KA, TP ACB with thermal overload and adjustable magnetic short-circuit releases g. 6 Nos. Current Transformer, ratio: 1600/5A with suitable accuracy and burden h. 6 Nos. Ammeter, 0 - 1250 A i. 2 No. Voltmeter, 0 - 500 V with selector switch j. 6 Nos. Phase Indicating Lamp <p><u>Outgoing:</u></p> <p>1 No. 1250A,50 KA, TP ACB with thermal overload and adjustable magnetic short-circuit release.</p>	
	<p>Any other changes at MDB panel equipment/ component shall be considered for proper load management/distribution.</p>	

8. 480 KVAR AUTOMATIC PFI PLANT		
Brand	To be mentioned (Preferably Circutor/ Schneider Electric/ Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<ul style="list-style-type: none"> a. Supply of assembled 16 SWG Sheet steel clad, Powder Coated, dust and vermin proof, free standing, floor mounting indoor Power Factor Plant. b. PFI of rating 480KVAR, 415V, 50Hz, three phase, with necessary hard drawn electrolytic drawn copper busbars, cable, control cable as per standard. c. All Capacitors with built-in direct discharge resistor <p>Any other changes at PFI shall be considered for proper solution.</p>	

9. LIGHTNING ARRESTOR		
Brand	To be mentioned	
Model	To be mentioned	

RESTRICTED

Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>Rated Voltage (RMS) : 9 kV Rated System voltage : 12 kV Frequency : 50 Hz Minimum Spark Over (RMS) : 14 kV Maximum Spark Over (RMS) : 40 kV Maximum Impulse Spark (Crest) : 45 kV Withstand Voltage -Wet , 10 sec. : 24 kV -Dry , 1 min. : 28 kV Discharge 33 kV (Crest) : 5 kA Impulse Current Withstand : 55 Ka</p> <p>Sufficient number of lightning arrestors shall be installed based on the substation design. In addition to mentioned rating, all other accessories required for this purpose shall be supplied by Bidder.</p>	

10. ATS panel-1250A		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>a. Automatic transfer switches of required number and rating considering above mentioned substation and generators shall be supplied and installed by the Bidder. b. The system will be connected with SCADA/DCIM monitoring system.</p>	
	<p>Incoming :</p> <p>a. 2No. 1250 A, 70 KA, TP ACB with thermal overload and adjustable magnetic short-circuit releases b. 6 Nos. Current Transformer, ratio: 1600/5A with suitable accuracy and</p>	

RESTRICTED

	<p style="text-align: center;">burden</p> <p>c. 6 Nos. Ammeter, 0 - 1250 A d. 2 No. Voltmeter, 0 - 500 V with selector switch e. 6 Nos. Phase Indicating Lamp</p> <p><u>Outgoing:</u></p> <p>2 No. 1250A,50 KA, TP ACB with thermal overload and adjustable magnetic short-circuit release.</p>	
--	--	--

11. BUS BAR TRUNKING SYSTEM(BBT)		
Brand	To be mentioned(Schneider/ Starline/Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	Bidder will plan, design, supply & install BBT system required at LT, HT & distribution up to Data center AVR for the smooth function.	

12. CABLES AND CONNECTIVITY		
General Features	<p>a. Required cables and connectivity for substation to be calculated and supplied.</p> <p>b. Maximum voltage drop shall be less than 2.5%.</p>	

13. EARTHING for Sub Station & Generator		
General Features	<p>a. For the protection of substation appropriate earthing technique to be applied.</p> <p>b. The earthing resistance will be less than 1 ohm.</p> <p>c. All substation unit/equipment shall be connected with earthing system to ensure substation protection.</p> <p>d. All DB shall be connected with the substation earthing system.</p>	

14. FIRE FIGHTING SYSTEM FOR SUB STATION		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>a. For the protection of substation required Sensors, detection system, fire suppression agent(Aerosol Spray or better solution) fire Port, panels, alarm system is to be supplied and installed.</p> <p>b. The system will be connected with SCADA/DCIM monitoring system.</p>	

15. FIRE FIGHTING SYSTEM for Generator Room		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>For the protection of Generator room from fire required Sensors, detection system, Foam fire suppression agent. Fire Port, panels, alarm system is to be supplied and installed.</p> <p>The system will be connected with SCADA/DCIM monitoring system.</p>	

16. Power system monitoring-SCADA System.		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	SCADA monitoring system will be established in power distribution network to monitor & control power distribution, to optimize overall network efficiency & to provide greater system reliability &	

RESTRICTED

	sustainability by real time visibility. All breakers, AC voltage sensor, temperature sensor have to be designed to monitor from Data Center/ Sub-Station from NOC.	
--	--	--

17. Infrastructure development for sub station & generator room.

General Features	The bidder will responsible for all civil works, utility power for sub-station, fire door, floor mat insulation, fencing for HV equipment, HT metering & RMU room, automatic shutter system etc.	
------------------	--	--

18. Lightning Protection System

Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of manufacturer	As per Tender Specification Article no 20	
General Features	<p>a. A lightning protection system includes a network of air terminals, bonding conductors, and ground electrodes designed to provide a low impedance path to ground for potential strikes.</p> <p>b. Required resistance <1 Ohm</p> <p>Grounding rods, inspection pit, lightning event counter have to be considered.</p>	

19. MISCELLANEOUS

General Features	Any other equipment/components required for operational activity of mentioned substation is to be supplied	
------------------	--	--

TENDER SPECIFICATION OF 350KVA DG SYSTEM CDC

Products Name/Items	Description of requirements	Bidder Response
20. 350KVA, GENERATOR		
Brand	To be mentioned (Preferably FG Wilson/ Perkins or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
Diesel Engine	<p><u>General</u> Diesel generator of required bhp, stationary types, four strokes with v cylinder arrangement shall be complete with integral air Intec with suitable air filter and exhaust system, speed regulator system, fuel injector system, lube oil system, silencers, self-containing piping, instruments, mounted on anti-vibration mountings and necessary equipment required.</p> <p><u>Type</u> Suitable for generating set application, turbo charged, multi cylinder,4-stroke, cold starting.</p> <p><u>Cycle</u> 4-stroke</p> <p><u>Speed</u> 1500 rpm</p> <p><u>Method of Starting</u> Battery</p> <p><u>Net Site Output</u> This shall be prime power output (exclusive of power requirement of auxiliaries deriving power with engines) at 1500 rpm. under site condition.</p> <p><u>Overload Feature</u> The engine shall be 10% overload capacity for one hour in every 12 hours of operation.</p> <p><u>Sound Silencer</u> Engine will be canopied and / or container type as appropriate considering customer installation site. The sound level of the supplied generator shall be 85db at 1 meter or better.</p>	

Products Name/Items	Description of requirements	Bidder Response
Engine Accessories	<p><u>Exhaust System</u></p> <ul style="list-style-type: none"> a. Each engine shall be provided with residential type silencers so as to limit the sound level from the DG set. Exhaust piping shall be fabricated from Class 'C' MS Black Pipe conforming to relevant IS standard size suitable to limit back pressure to within permissible limit. b. The exhaust shall be terminated as per pollution norms. Exhaust piping inside DG room shall be insulated with 75 mm thick mineral wool and 26 gauge Al. cladding or as applicable. c. Exhaust piping shall be connected to the engine by means of flexible section or an expansion joint. <p><u>Turbocharger</u></p> <ul style="list-style-type: none"> a. Turbocharger mounted at the side of the engine for better conversion of energy of exhaust gases resulting in more power, improved fuel economy, altitude compensation, lower exhaust temperature, lower smoke and noise level. <p><u>Air Filter</u></p> <ul style="list-style-type: none"> a. The engine air intake shall be fitted with dry type air cleaner with vacuum indicator facilitating change of air filter. <p><u>Lubricating Oil System</u></p> <ul style="list-style-type: none"> a. The engine shall be of the totally enclosed type and fitted with a positive pressure system of lubrication to all working parts. b. Lubricating oil shall be circulated in the engine by an engine driven pump. There shall be no moving part requiring lubrication by hand prior to the starting of the engine or while in operation. It shall be so designed that when the engine starts after a long shut down lubrication failure does not occur. c. Necessary priming pump for the lube oil circuit shall be installed to keep bearings primed. 	

Products Name/Items	Description of requirements	Bidder Response
	<p><u>Safety Controls</u></p> <p>a. Low Lubricating Oil Pressure : Pressure sensors shall be fitted such that in the event of a fall in the lube oil pressure and indication shall be actuated. In addition, the engine shall be automatically shut down in the event of lube oil pressure dropping to a pre-determined low value.</p> <p>b. Over Speed: Speed control shall be so arranged that 12-13% increase over normal rated speed shall cut off fuel supply, thus stopping the engine.</p> <p>c. Engine Mounted Instruments Panel (Electronic : The flexibly mounted instrument panel on engine shall be complete with the following Digital Display to indicate :</p> <ul style="list-style-type: none"> • Coolant Temperature • Lub Oil Pressure • Battery voltage • Engine speed • Engine Run hours <p>d. Engine and alternator protection:</p> <ul style="list-style-type: none"> • High Coolant Temperature • Over-speed • Low lube oil pressure <p>The DG Set shall be supplied with micro-processor based generator monitoring, metering & protection features like :</p> <ul style="list-style-type: none"> • Analogue & Digital AC output metering • Battery monitoring system to sense and warn against a weak battery condition. • Digital alarm & status message display • Overload • Over current • Over voltage • Under voltage • Over frequency • Under frequency 	

Products Name/Items	Description of requirements	Bidder Response
Alternator	<p><u>General</u></p> <p>a. Synchronous alternator of suitable capacity to generate 350 KVA output at alternator terminal at 415 V, 50 Hz, 3 Phase, 4 Wire, 0.8 pf (lag) 1500 rpm and in accordance with BS:2613 / IS:4722/IEC- 34(Part-I) and self air-cooled type driven by the Diesel Engine.</p> <p>b. Generator / Alternator shall have following characteristics:</p> <p>b.1 Permissible voltage regulation (max.) in static condition + 0.5%</p> <p>b.2 Permissible over load of 10% for one hour in every 12 hrs. of operation</p> <p>b.3 Permissible voltage & frequency variation of + 0.5% & + 1 % respectively</p> <p><u>Excitation System</u> The Generator shall be provided with brush less excitation system capable of supplying the excitation current of the generator under all conditions of output from no load to full load.</p> <p><u>Battery</u> Battery of voltage and capacity compatible with the engine, complete with battery charging equipment shall be provided to energize electric starting equipment. Batteries shall be of lead-acid automotive type. The charging unit shall be part of DG control panel.</p> <p><u>DG Set Accessories</u> Any other item not specifically mentioned but required for satisfactory installation, operation and maintenance of DG Set shall be supplied by the Bidder.</p>	
DRAWINGS AND DATA	<p>Drawings and Data shall be provided that includes:</p> <p>a. DG Set layout, showing exhausts piping, typical supporting arrangement for all piping & exhaust system.</p> <p>b. P&I diagram for Cooling System & Fuel oil supply system</p>	
TESTS AT	The following tests shall be performed at	

Products Name/Items	Description of requirements	Bidder Response
MANUFACTURER'S SITE	<p>manufacture's site prior to packing and dispatch.</p> <p><u>On DG Set</u></p> <ol style="list-style-type: none"> Maximum power load capacity. Maximum motor starting capacity Endurance test. Fuel consumption at full load, 50% load, 75% load and 25% load. <p><u>On The Alternator</u></p> <ol style="list-style-type: none"> High voltage tests on stator and rotor windings. Insulation resistance of stator and rotor windings. Temperature rise test. Stator voltage and current tests. Stator phase sequence check. <p><u>On The Exciter</u></p> <ol style="list-style-type: none"> High voltage tests on stator and rotor winding. Insulation resistance of stator and rotor windings. Temperature rise test. Measurement of losses. <p><u>On The Automatic Voltage Regulator</u></p> <ol style="list-style-type: none"> Sensitivity test. Response time test. <p>All routine test as per IS/BS codes shall be conducted on alternator, exciter and AVR. Moreover the engine and alternator supplied shall be duly tested and supported by the test certificates of the respective manufacturer.</p>	
DRAWING & DOCUMENTATION TO BE SUBMITTED	<p>Following information and documentations to be provided:</p> <ol style="list-style-type: none"> Electrical layout drawing showing location of equipment, cable routing, bus duct connections, fuel piping arrangement with fuel tank for DG Set, exhaust system etc. Plan & Elevation drawing including sectional details. Single Line Diagram showing rating of components, metering and protection for DG Panel/PLC Panel/Distribution boards etc. Earthing layout showing connections to DG, panels Wiring Diagram. 	

Products Name/Items	Description of requirements	Bidder Response
	<p>f. Write-up on control philosophy for complete emergency electrical system containing starting & stopping sequence, interlocks, metering, annunciation etc.</p> <p>g. All required drawings/ documents/ technical information required during various stages of works shall be submitted as and when required.</p> <p>h. All drawings submitted shall be in sufficient detail to indicate the type, size, general arrangement & foundation drawing, weight, the external connections, fixing arrangement required, the dimensions required for installation and interconnections with other equipment and materials, clearances and space required between various portions of equipment and any other information specifically requested.</p>	

21. Day Tank for Fuel of Generator

General Features	Bidder will propose & design 500litter Day Tank of Fuel for 350KVA Generator. The tank should come with all necessary sensors to connect with SCADA system.	
------------------	---	--

22. Auto fuel refill system

General Features	Bidder will propose & design automatic fueling system for 2nos generator, this system will include under ground fuel reservoir, ready to use day tank, necessary piping, electric pump & motor, necessary sensors, control & monitoring system. System will be integrated with Sub Station SCADA monitoring system.	
------------------	---	--

23. Underground fuel reserve tank

General Features	The underground fuel reserve tank capacity will be 10000litter for 2nos 350KVA Generator.	
------------------	---	--

DRDC PASSIVE EQUIPMENT FOR SUB-STATION

<u>TENDER SPECIFICATION OF 500KVA SUB STATION DRDC</u>		
Products Names/Items	Description of requirements	Bidder Response
1. Express Line Feeder with RMU & HT Metering Panel		
General Requirements	For 500KVA substation the express line feeder from nearby RMU (or with RMU if required), HT Metering panel shall be required. Bidder will coordinate with local power supply authority and will plan and propose accordingly.	

2. 11kv Isolator with Vacuum Contactor		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	Rated Current: 630 Amps Voltage Rating: 11kV (or as specified based on system requirements) Short-Circuit Rating: Ensure compatibility with system short-circuit requirements, typically around 25kA or as specified. Mounting: Indoor, Floor-mounted as per substation design. Type: 11KV Isolator with vacuum contactor Standards Compliance: Must comply with IEC 62271-102 for high-voltage switchgear and control gear isolators. Protection Class: IP54 or IP65, depending on environmental exposure and dust/moisture levels.	

3. HT Automatic Voltage Regulator (AVR) with Bypass Arrangement		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	a. The HT Automatic Voltage Regulator/Controller (HT AVR) shall be 11KV copper wound suitable for input voltage range from	

RESTRICTED

	<p>8 KV to 12KV with output stabilized at 11 KV + 1%, indoor, oil-immersed, naturally cooled, on load, step less type with rolling contacts.</p> <p>b. The principle of operation of HT AVR shall be auto transformer, tapped continuously with the aid of rolling contact mechanism moved by self-powered FHP synchronous motor for stabilizing output voltage automatically.</p> <p>c. Correction of voltage shall also be possible by motor through push buttons. If Automatic and motorized control become defunct, correction of voltage shall be possible by means of a hand wheel.</p>	
Standards:	The HT AVR shall conform to the relevant BS/IS specification with upto date amendments	
Power supply parameters:	<p>a. The HT AVR shall be capable of continuous operation as specified rating.</p> <p>b. The HT AVR shall be designed to give stabilized output voltage at 11000 V + 1%, 3 Phase, 50 Hz, suitable for balanced input & unbalanced load, when the input voltage varies between 8000 V to 12000 V, 3 phase, 50 Hz. On 11 KV 3 phase, 50 Hz. System.</p>	

4. 11 KV H.T Switchgear (VCB)		
Quantity: 1		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>11 KV H.T. SWITCHGEAR (630 A, VCB) Sheet steel clad 14 SWG, Powder Coated dust and vermin proof, freestanding, floor mounting indoor HT Switchgear 11KV, 50Hz, three phase, 800 A hard drawn electrolytic copper busbars equipped with:</p> <p>a) 1 No. 630 A, 11 KV, breaking current 25KA (3 sec.), making current 50 KA, 50 Hz, TP Vacuum Circuit Breaker (Fixed Type) with motor operated mechanism with closing solenoid shunt releases, auxiliary contacts 5NO + 5NC and limit switch (1 'NO + 1 NC) for indication "Closing spring charged". mechanical on/off/trip indicator. Origin : To be mention by bidder</p>	

	<p>b) 3 Nos. Cast resin insulated, double pole, Potential Transformer, ratio: $11\sqrt{3}/.11/\sqrt{3}$ KV, Class 0.5, 50 VA, Origin : To be mention by bidder</p> <p>c) 1 No. MCB of adequate rating for PT Secondary Protection.</p> <p>d) 3 Nos. Cast resin insulated, 11 KV dry type double 'core CT with Ratio: 60/5/5A, 1st core for metering, 2nd for protection Core 1 : 10 VA, Class 0.5M5 Core 2 : 15 VA, Class 10P10 Origin : To be mention by bidder.</p> <p>e) 3 Nos. Digital Ammeter, 0 - 60 A. 1 No. Digital Voltmeter, 0 - 15 KV, with selector switch 1 No. Triple pole IDMT Solid State type Relay for over current, Earthfault and short circuit protection, Control voltage - 110 V DC Origin : To be mention by bidder.</p> <p>f) 2 Nos. ON and OFF/TRIP Push Button 2 Nos. Indicating Lamps ON and OFF/TRIP 1 No. Panel Heater</p> <p>Any other changes at HT panel equipment/ component shall be considered for proper load management/distribution.</p>	
--	--	--

5. Cast Resin Dry Type Transformer(500kva)		
Brand	To be mentioned (Preferably Schneider/Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	500kVA, 11/0.415kV Cast Resin Dry Type Transformer with Canopy Three phased cast resin dry transformers, class F1, E2, C2, indoor use, with standard accessories. Design manufacturing, routine tests & tolerances according to IEC 60076-11 standards. Standard fittings: 4 flat bi-directional rollers. 2 lifting lugs 2 earthing points.	

RESTRICTED

	<p>1 rating plate(on HV side) HV/ LV connections: Connection from top onto flat bar terminals. Enclosure: IP31 Quality Assurance: Transformer shall be made according to system of quality assurance with (quality assurance in design, production and servicing) standards ISO 9001, certificate AFAQ bn 1993/1275</p>	
<p>Technical Data:</p>	<ol style="list-style-type: none"> 1. Rated power: 500KVA 2. Rated frequency: 50Hz 3. Rated lightning impulse withstand voltage BIL 1.2/ 50µs HV :75kV peak LV :8kV peak 4. Rated power frequency withstand voltage 50Hz 1mn HV :28kV rms LV :3kV rms 5. Rated insulation level HV :12kV LV :1.1kV 6. Rated voltage Primary :11kV Secondary at no load : 0.415kV 7. Tap changer links (in HV winding): Type Off load in tapping range : % +5 to -5 Per step size : 2.50% Step/ Position No. : 5-Apr 8. Vector group : Dyn11 9. Maximum ambient temperature : 40°C 10. Maximum installation altitude above sea level: 1000m 11. Cooling System: AN 12. Installation: Indoor 13. Winding Material: HV/ LV (As per industry standard) 14. Loss: No load loss: 900W Load loss at 75°C: 6020W 15. Rated impedance voltage at 75°C: 5% 16. Thermal class insulation: Class F 17. Temperature rise: 100K 18. Acoustic power LwA: 69dB (A) 19. Acoustic pressure LPA at 1.00m: 56dB (A) <p>Raw Materials: A) Brand: To be mentioned. B) Model: To be mentioned.</p>	

RESTRICTED

	C)COO: To be mentioned. D) COM: To be mentioned.	
TESTS AT MANUFACTURER'S SITE	The following tests shall be performed at manufacture's site prior to packing and dispatch. a.No Load loss b.No load excitation current c.Load losses and impedance voltage d.Dielectric tests e.Switching impulse test f.Lightning impulse test g.Partial discharge test h.Insulation power factor i.Noise measurement j.Temperature rise (Heat run) Short circuit test	

6. Phase Correction Device (PCD)-800A		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<ul style="list-style-type: none"> a. 16 SWG sheet steel enclosed, type tested, dust and vermin proof, free standing floor stand indoor type, powder coated paint finished. b. The PCD busbar will be hard drawn electrolytic required Amp copper busbar, properly insulated. c. TPN & E equipped with insulator, internal cover for busbar section. d. Digital multimeter to show 3 phase's volts, amp, etc.; indicator lamp-3pcs per phase, phasing preventor relay 3 pcs for phase correction; AC electronic Relay 3 pcs, DC electronic relay - 3 pcs, timer Second -6 pcs. e. During design bidder will consider appropriate bus bar, breaker, protection devices, monitoring devices for SCADA/DCIM monitoring. f. Fully automatic phase reversal correction. Load Protection from High or Low voltage. g. Selectable switch for high and low voltage selection. h. Nominal voltage will be minimum 400V. Nominal operating current will be 1600A or as required to construct the data center. 	

	i.	
--	----	--

7. LT Switchgear-800A & 1XMDB-500A, MCCB		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>Incoming :</p> <ul style="list-style-type: none"> a. 1 No. 800 A, 70 KA, TP MCCB with thermal overload and adjustable magnetic short-circuit releases b. 3 Nos. Current Transformer, ratio: 800/5A with suitable accuracy and burden c. 3 Nos. Ammeter, 0 - 1600 A d. 1 No. Voltmeter, 0 - 500 V with selector switch e. 3 Nos. Phase Indicating Lamp <p><u>Outgoing:</u></p> <p>2 No. 800A,50 KA, TP MCCB with thermal overload and adjustable magnetic short-circuit release.</p> <p>Any other changes at LT panel equipment/ component shall be considered for proper load management/distribution.</p>	
General Features of MDB 1&2	<p>Incoming :</p> <ul style="list-style-type: none"> f. 1No. 500 A, 70 KA, TP MCCB with thermal overload and adjustable magnetic short-circuit releases g. 3 Nos. Current Transformer, ratio: 500/5A with suitable accuracy and burden h. 6 Nos. Ammeter, 0 - 1250 A i. 1 No. Voltmeter, 0 - 500 V with selector switch j. 3 Nos. Phase Indicating Lamp <p><u>Outgoing:</u></p> <p>2 No. 500A,50 KA, TP MCCB with thermal overload and adjustable magnetic short-circuit release.</p>	

8. 300 KVAR Automatic PFI Plant		
Quantity: 1		
Brand	To be mentioned (Preferably Circutor/ Schneider Electric/ Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>a. Supply of assembled 16 SWG Sheet steel clad, Powder Coated, dust and vermin proof, free standing, floor mounting indoor Power Factor Plant.</p> <p>b. PFI of rating 300KVAR, 415V, 50Hz, three phase, with necessary hard drawn electrolytic drawn copper busbars, cable, control cable as per standard.</p> <p>c. All Capacitors with built-in direct discharge resister</p> <p>Any other changes at PFI shall be considered for proper solution.</p>	

9. Lightning Arrestor		
Quantity: 1Set		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>Rated Voltage (RMS) : 9 kV Rated System voltage : 12 kV Frequency : 50 Hz Minimum Spark Over (RMS) : 14 kV Maximum Spark Over (RMS) : 40 kV Maximum Impulse Spark (Crest) : 45 kV Withstand Voltage -Wet , 10 sec. : 24 kV -Dry , 1 min. : 28 kV Discharge 33 kV (Crest) : 5 kA Impulse Current Withstand : 55 Ka</p> <p>Sufficient number of lightning arrestors shall be installed based on the substation design. In addition to mentioned rating, all other accessories required for this purpose shall be supplied by Bidder.</p>	
10. Automatic Transfer Switch (ATS)-500A		
Brand	To be mentioned	

RESTRICTED

Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	Automatic transfer switches of required number and rating considering above mentioned substation and generators shall be supplied and installed by the Bidder.	

11. Cables And Connectivity

11. Cables And Connectivity		
General Features	<ul style="list-style-type: none"> a. Required cables and connectivity for substation to be calculated and supplied. b. Maximum voltage drop shall be less than 2.5%. 	

12. Earthing & Bonding

12. Earthing & Bonding		
General Features	<ul style="list-style-type: none"> a. For the protection of substation appropriate earthing technique to be applied. b. The earthing resistance will be less than 1 ohm. c. All substation unit/equipment shall be connected with earthing system to ensure substation protection. d. All DB shall be connected with the substation earthing system. 	

13. Fire Fighting System for Sub Station

13. Fire Fighting System for Sub Station		
Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<ul style="list-style-type: none"> a. For the protection of substation required Sensors, detection system, fire suppression agent(Aerosol Spray or better solution) fire Port, panels, alarm system is to be supplied and installed. b. The system will be connected with SCADA/DCIM monitoring system. 	

14. Fire Fighting System for Generator Room

14. Fire Fighting System for Generator Room		
Brand	To be mentioned	

RESTRICTED

Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>a. For the protection of substation required Sensors, detection system, fire suppression agent (Foam fire suppression agent or better solution) fire Port, panels, alarm system is to be supplied and installed.</p> <p>b. The system will be connected with SCADA/DCIM monitoring system.</p>	

15. Power system monitoring-SCADA System

Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
General Features	<p>a. SCADA monitoring system has to be established in power distribution network to monitor & control power distribution, to optimize overall network efficiency & to provide greater system reliability & sustainability with real time visibility.</p> <p>b. All breakers, AC voltage sensor, temperature sensor have to be designed to monitor Data Center/ Sub-Station from NOC.</p>	

16. Infrastructure Development work for Sub Station & Generator

General Features	The bidder is responsible for all civil works, utility power for sub-station, fire door, floormate insulation, fencing for HV equipment, HT metering, RMU room, automatic shutter system etc.	
------------------	---	--

17. Lightning Protection System

Brand	To be mentioned	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Country of	As per Tender Specification Article no 20	

RESTRICTED

manufacturer		
General Features	<p>a. A lightning protection system includes a network of air terminals, bonding conductors, and ground electrodes designed to provide a low impedance path to ground for potential strikes.</p> <p>b. Required resistance <1 Ohm Grounding rods, inspection pit, lightning event counter have to be considered.</p>	

18. Miscellaneous		
General Features	Any other equipment/components required for operational activity of mentioned substation is to be supplied	

19. 250KVA, GENERATOR		
Brand	To be mentioned (Preferably FG Wilson/ Perkins or Equivalent)	
Model	To be mentioned	
Country of origin	As per Tender Specification Article no 20	
Manufacturing Country	As per Tender Specification Article no 20	
Diesel Engine	<p><u>General</u> Diesel generator of required bhp, stationary types, four strokes with v cylinder arrangement shall be complete with integral air Intec with suitable air filter and exhaust system, speed regulator system, fuel injector system, lube oil system, silencers, self-containing piping, instruments, mounted on anti-vibration mountings and necessary equipment required.</p> <p><u>Type</u> Suitable for generating set application, turbo charged, multi cylinder,4-stroke, cold starting.</p> <p><u>Cycle</u> 4-stroke</p> <p><u>Speed</u> 1500 rpm <u>Method of Starting</u> Battery</p> <p><u>Net Site Output</u> This shall be prime power output (exclusive of power requirement of auxiliaries deriving power with engines) at 1500 rpm. under site condition.</p> <p><u>Overload Feature</u> The engine shall be 10% overload capacity for one hour in every 12 hours of operation.</p> <p><u>Sound Silencer</u> Engine will be canopied and / or container type as appropriate considering customer</p>	

	<p>installation site. The sound level of the supplied generator shall be 85db at 1 meter or better.</p>	
<p>Engine Accessories</p>	<p><u>Exhaust System</u></p> <ul style="list-style-type: none"> a. Each engine shall be provided with residential type silencers so as to limit the sound level from the DG set. Exhaust piping shall be fabricated from Class 'C' MS Black Pipe conforming to relevant IS standard size suitable to limit back pressure to within permissible limit. b. The exhaust shall be terminated as per pollution norms. Exhaust piping inside DG room shall be insulated with 75 mm thick mineral wool and 26 gauge Al. cladding or as applicable. c. Exhaust piping shall be connected to the engine by means of flexible section or an expansion joint. <p><u>Turbocharger</u></p> <ul style="list-style-type: none"> a. Turbocharger mounted at the side of the engine for better conversion of energy of exhaust gases resulting in more power, improved fuel economy, altitude compensation, lower exhaust temperature, lower smoke and noise level. <p><u>Air Filter</u></p> <ul style="list-style-type: none"> a. The engine air intake shall be fitted with dry type air cleaner with vacuum indicator facilitating change of air filter. <p><u>Lubricating Oil System</u></p> <ul style="list-style-type: none"> a. The engine shall be of the totally enclosed type and fitted with a positive pressure system of lubrication to all working parts. b. Lubricating oil shall be circulated in the engine by an engine driven pump. There shall be no moving part requiring lubrication by hand prior to the starting of the engine or while in operation. It shall be so designed that when the engine starts after a long shut down lubrication failure does not occur. c. Necessary priming pump for the lube oil circuit shall be installed to keep bearings primed. <p><u>Safety Controls</u></p> <ul style="list-style-type: none"> a. Low Lubricating Oil Pressure: Pressure sensors shall be fitted such that in the event of 	

	<p>a fall in the lube oil pressure and indication shall be actuated. In addition, the engine shall be automatically shut down in the event of lube oil pressure dropping to a pre-determined low value.</p> <p>b. Over Speed: Speed control shall be so arranged that 12-13% increase over normal rated speed shall cut off fuel supply, thus stopping the engine.</p> <p>c. Engine Mounted Instruments Panel (Electronic: The flexibly mounted instrument panel on engine shall be complete with the following Digital Display to indicate:</p> <ul style="list-style-type: none"> • Coolant Temperature • Lub Oil Pressure • Battery voltage • Engine speed • Engine Run hours <p>d. Engine and alternator protection:</p> <ul style="list-style-type: none"> • High Coolant Temperature • Over-speed • Low lube oil pressure <p>The DG Set shall be supplied with micro-processor based generator monitoring, metering & protection features like :</p> <ul style="list-style-type: none"> • Analogue & Digital AC output metering • Battery monitoring system to sense and warn against a weak battery condition. • Digital alarm & status message display • Overload • Over current • Over voltage • Under voltage • Over frequency • Under frequency 	
Alternator	<p><u>General</u></p> <p>a. Synchronous alternator of suitable capacity to generate 250 KVA output at alternator terminal at 415 V, 50 Hz, 3 Phase, 4 Wire, 0.8 pf (lag) 1500 rpm and in accordance with BS:2613 / IS:4722/IEC- 34(Part-I) and self air-cooled type driven by the Diesel Engine.</p> <p>b. Generator / Alternator shall have following characteristics:</p> <p style="padding-left: 20px;">b.1 Permissible voltage regulation (max.) in static condition + 0.5%</p> <p style="padding-left: 20px;">b.2 Permissible over load of 10% for one hour in every 12 hrs. of operation</p>	

	<p>b.3 Permissible voltage & frequency variation of + 0.5% & + 1 % respectively</p> <p><u>Excitation System</u> The Generator shall be provided with brush less excitation system capable of supplying the excitation current of the generator under all conditions of output from no load to full load.</p> <p><u>Battery</u> Battery of voltage and capacity compatible with the engine, complete with battery charging equipment shall be provided to energize electric starting equipment. Batteries shall be of lead-acid automotive type. The charging unit shall be part of DG control panel.</p> <p><u>DG Set Accessories</u> Any other item not specifically mentioned but required for satisfactory installation, operation and maintenance of DG Set shall be supplied by the Bidder.</p>	
<p>DRAWINGS AND DATA</p>	<p>Drawings and Data shall be provided that includes:</p> <ul style="list-style-type: none"> a. DG Set layout, showing exhausts piping, typical supporting arrangement for all piping & exhaust system. b. P&I diagram for Cooling System & Fuel oil supply system 	
<p>TESTS AT MANUFACTURER'S SITE</p>	<p>The following tests shall be performed at manufacture's site prior to packing and dispatch.</p> <p><u>On DG Set</u></p> <ul style="list-style-type: none"> a. Maximum power load capacity. b. Maximum motor starting capacity c. Endurance test. d. Fuel consumption at full load, 50% load, 75% load and 25% load. <p><u>On The Alternator</u></p> <ul style="list-style-type: none"> a. High voltage tests on stator and rotor windings. b. Insulation resistance of stator and rotor windings. c. Temperature rise test. d. Stator voltage and current tests. e. Stator phase sequence check. <p><u>On The Exciter</u></p> <ul style="list-style-type: none"> a. High voltage tests on stator and rotor winding. b. Insulation resistance of stator and rotor windings. c. Temperature rise test. d. Measurement of losses. <p><u>On The Automatic Voltage Regulator</u></p> <ul style="list-style-type: none"> a. Sensitivity test. b. Response time test. <p>All routine test as per IS/BS codes shall be conducted</p>	

RESTRICTED

	<p>on alternator, exciter and AVR. Moreover the engine and alternator supplied shall be duly tested and supported by the test certificates of the respective manufacturer.</p>	
<p>DRAWING & DOCUMENTATION TO BE SUBMITTED</p>	<p>Following information and documentations to be provided:</p> <ul style="list-style-type: none"> a. Electrical layout drawing showing location of equipment, cable routing, bus duct connections, fuel piping arrangement with fuel tank for DG Set, exhaust system etc. b. Plan & Elevation drawing including sectional details. c. Single Line Diagram showing rating of components, metering and protection for DG Panel/PLC Panel/Distribution boards etc. d. Earthing layout showing connections to DG, panels e. Wiring Diagram. f. Write-up on control philosophy for complete emergency electrical system containing starting & stopping sequence, interlocks, metering, annunciation etc. g. All required drawings/ documents/ technical information required during various stages of works shall be submitted as and when required. h. All drawings submitted shall be in sufficient detail to indicate the type, size, general arrangement & foundation drawing, weight, the external connections, fixing arrangement required, the dimensions required for installation and interconnections with other equipment and materials, clearances and space required between various portions of equipment and any other information specifically requested. 	

20. Day Tank for Fuel of Generator

<p>General Features</p>	<p>Bidder will propose & design 500litter Day Tank of Fuel for 250KVA Generator. The tank should come with all necessary sensors to connect with SCADA system.</p>	
-------------------------	--	--

TECHNICAL SPECIFICATION OF INFRASTRUCTURE DEVELOPMENT WORKS- CDC

Infrastructure Development, Furniture & fixture and related interior decoration (Infrastructure Developments)		
(Qty: 1 Set)		
Features List	Features Description	Remarks
Brand	To be mentioned	
Model No.	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Total Floor Space	Bidder will propose as per design & requirement.	
Infrastructure Development	As per proposed design by the bidder approved by BNNET acceptance team.	
Glass Partition	As per proposed design by the bidder approved by BNNET acceptance team.	
Glass Door	As per proposed design by the bidder approved by BNNET acceptance team.	
Cable Containment & Infrastructure Work.	As per proposed design by the bidder approved by BNNET acceptance team.	
Raised Floor	As per proposed design by the bidder approved by BNNET acceptance team.	
Brick work	Bidder will complete all short of brick works as per design.	
Base Elevation for chiller installation	As per proposed design by the bidder approved by BNNET acceptance team.	
Plaster & paint work	Bidder will complete all short of plaster & paint works as per design.	
Tiles work	Bidder will complete all short of tiles works as per design.	
Interior design & Furniture	Bidder will propose all short of Interior design & Furniture works as per BNNET supplied draft design with required modification by the bidder & approved by the BNNET acceptance team.	
Chair	a) Class room – 13 nos	
	b) OIC room – 3 nos	
	c) Meeting room – 7 nos	
	d) COMMANDANT BN NET – 3 nos	
	e) PS OF COMMANDANT -1 nos	

RESTRICTED

	f) OFFICER'S ROOM – 9 nos	
	g) STAFF ROOM – 6 nos	
	h) Forensic Lab – 6 nos	
	i) STAGGING ROOM' – 3 nos	
	j) SOC Room – 6 nos	
	k) NOC Room – 8 nos	
Table Single	a) Class room – 13 nos	
	b) Meeting room – 6 nos	
	c) COMMANDANT BN NET – 3 nos	
	d) PS OF COMMANDANT -1 nos	
	e) STAFF ROOM – 6 nos	
	f) Forensic Lab – 6 nos	
	g) STAGGING ROOM' – 3 nos	
	h) SOC Room – 6 nos	
	i) NOC Room – 8 nos	
Table executive	a) OIC room – 1nos	
	b) COMMANDANT BN NET – 1 nos	
	c) OFFICER'S ROOM – 3 nos	
Washroom	a) COMMANDANT BN NET – 1 nos	
	b) OFFICER'S ROOM – 1 nos	
Full height cabinet	a) COMMANDANT BN NET – 1 nos	
Low height cabinet	a) OFFICER'S ROOM – 3 nos	
	b) STAFF ROOM – 3 nos	
	c) COMMANDANT BN NET – 1 nos	
	d) PS OF COMMANDANT -1 nos	
	e) Forensic Lab – 3 nos	
	f) STAGGING ROOM' – 1 nos	
	g) SOC Room – 3 nos	
	h) NOC Room – 1 nos	
Wash room	a) STAGGING ROOM' – 1 nos	
	b) OFFICER'S ROOM – 1 nos	
Ramp	Bidder will propose all short of Ramp works as per design.	
Signage	Bidder will propose all short of signage work as per design	
Reception area work	Bidder will propose all short of Reception area work as per design.	
Chiller Shade	Chiller shade to be constructed with all utility connections	

RESTRICTED

	by the bidder at ground floor of CDC building. The Generators and Sub-stations shall be installed in the ground floor. The underground oil reserve tank shall be constructed near to the generator installation site. The bidder may collect requirement drawing from End User (DNIT, NHQ). The bidder has to conduct site survey in-details and submit layout along with 3D design with the offer. The cost is to be included in the heading of infrastructure development cost separately	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	

Note: All chair & table need to be approved by BNNET acceptance team before delivery. Moreover, the actual picture of the items needs to be submitted with the offer in the technical part.

TECHNICAL SPECIFICATION OF INFRASTRUCTURE DEVELOPMENTS- DRDC

Infrastructure Development, Furniture & fixture and related interior decoration (Infrastructure Developments)		
(Qty: 1 Set)		
Features List	Features Description	Remarks
Brand	To be mentioned	
Model No.	To be mentioned	
Country of Origin	As per tender specification, article 20	
Country of Manufacture	As per tender specification, article 20	
Total Floor Space	Bidder will propose as per design & requirement.	
Infrastructure Development	As per proposed design by the bidder approved by BNNET acceptance team.	
Glass Partition	As per proposed design by the bidder approved by BNNET acceptance team.	
Glass Door	As per proposed design by the bidder approved by BNNET acceptance team.	
Data Center Infrastructure Work	As per proposed design by the bidder approved by BNNET acceptance team.	
Cable Containment & Infrastructure	As per proposed design by the bidder approved by BNNET acceptance team.	
Raised Floor	As per proposed design by the bidder approved by BNNET acceptance team.	
Pre fabricated building for genset & Substation (2nd storied building, size: 800 sft in each floor)	As per proposed design by the bidder approved by BNNET acceptance team.	
Brick work	Bidder will complete all short of brick works as per design.	
Plaster & paint work	Bidder will complete all short of plaster & paint works as per design.	
Tiles work	Bidder will complete all short of tiles works as per design.	
Interior design & Furniture	Bidder will propose all short of Interior design & Furniture works as per BNNET supplied draft design with required modification by the bidder & approved by the BNNET acceptance team.	

RESTRICTED

Chair	a) OIC room – 3 nos	
	b) Meeting room – 7 nos	
	c) OFFICER'S ROOM – 9 nos	
	d) STAFF ROOM – 6 nos	
	e) NOC Room – 8 nos	
Table Single	a) Meeting room – 6 nos	
	b) STAFF ROOM – 6 nos	
	c) NOC Room – 8 nos	
Table executive	a) OIC room – 1nos	
	b) OFFICER'S ROOM – 3 nos	
Low height cabinet	a) OFFICER'S ROOM – 3 nos	
	b) STAFF ROOM – 3 nos	
	c) NOC Room – 1 nos	
Ramp	Bidder will propose all short of Ramp works as per design.	
Signage	Bidder will propose all short of signage work as per design	
Reception area work	Bidder will propose all short of Reception area work as per design.	
Generator & Substation Shade	Generator & Substation shade to be constructed with all utility connections by the bidder at ground floor/nearby place selected by BN NAVY CTG of DRDC. The Generators shall be installed in Ground Floor and Substations shall be installed in the 1 st floor. The bidder may collect requirement drawing from End User (DNIT, NHQ). The bidder has to conduct site survey in-details and submit layout along with 3D design with the offer. The cost is to be included in the heading of infrastructure development cost separately	
BOM	BOM to be attached with technical compliance of each item	
Product Brochure	Product Brochure to be attached with technical compliance of each item	

Note: All chair & table need to be approved by BNNET acceptance team before delivery. Moreover, the actual picture of the items needs to be submitted with the offer in the technical part.

**TECHNICAL SPECIFICATIONS: STRUCTURED CABLING SYSTEM FOR
DATA CENTER (CDC, DRDC & NHQ DC)**

Fiber & Copper Cabling Solution – Generic requirement

S. No	Min Specification	Bidders Response	Remarks
1	The offered MPO OM4 system should be low loss to support the below listed applications under given configuration – <i>MPO system shall support upto 6 connections in a single channel and meet the following application loss and length limits:</i> <ul style="list-style-type: none"> • 10GBASE-S upto 350m • 40G BiDi upto 120m • 8G FC at 850nm upto 150m • 16F FC at 850nm upto 100m • 32G FC at 850nm upto 80m 		
3	<i>For flexibility in design and future upgrades the MPO system shall support Max attenuation of $\leq 2.40\text{dB}@850\text{nm}$ for 6 connector MPO channel segment upto 50mtr length.</i>		
5	Documentary proof must be submitted from OEM in support of these applications under 6 connector MPO configurations.		
6	The Cat6A cable must be tested by Intertek test facility to the following standards: <ul style="list-style-type: none"> - ANSI/TIA 568.2-D: Category 6A Channel – 4 connector - IEEE 802.3bt (Type 4) for 4PPoE upto 60 deg C 3rd Party verification for Short Channel (15m) testing must be provided as part of the bid response. Copies of test reports should be appended to this RFP.		
7	All components for MM fiber, CAT6A copper cabling, AIM system components, including copper and fiber pathway systems must be from any single OEM.		
8	The passive cabling OEM shall have ISO 9001, 14001 & 45001 certified manufacturing facility of their own.		
9	All copper cables and trunk cords used inside the DC must be LSZH IEC 60332-3 (Flame test), IEC 61034-2 (Smoke density test), IEC 60754-2 (toxic gas emission test)		

	compliant and CPR rated as Dca or better as per EN50575 standard.		
--	---	--	--

Cat6A UTP Cabling Systems

1. CAT 6A UTP LSZH Cable, Box of 305 mtr

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	CAT6A U/UTP 23 AWG Cable should be ETL Verified to ANSI/TIA 568.2-D Category 6A and ISO/IEC 11801 Class EA Specifications.	
	Cable shall be constructed with pair separator as well as individual conductor separator for superior ANEXT performance under CAT6A channel.	
	Electrical properties:	
	Max DC Resistance: ≤ 7.61 Ohms/100m	
	Max. Operating voltage: 80 V	
	Frequency: up to 550 Mhz	
	The cable shall have Low-Smoke, Zero Halogen (LSZH) jacketing and must comply with the following Fire Safety standards: 1) ISO/IEC 60332-3-22: Vertical Flame Spread 2) ISO/IEC 60754-2: Acidity 3) ISO/IEC 61034-2: Smoke Density	
	Cable shall be compliant to EN50575 CPR Cable Euro Class and certified for Dca or better standards. Certificate should be submitted with bid.	
	Certifications and Test Reports:	
	Category 6A cable alongwith offered channel components should be certified by Intertek lab under 4 connector channel configuration to the requirement of ANSI/TIA 568-C.2 for short links (<15m) as required for data centers. Test Certificates to be provided with bid.	
	CAT6A Cable must be certified for IEEE 802.3bt Type 4 transmission for remote powering (4PPoE) upto 60 Deg C.	

2. CAT6A UTP Patch Panel 24 port loaded intelligent Ready

Feature List	Feature Description	Bidders Response

Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	CAT6A UTP Patch Panel 24 port loaded, 1U with front patch cord manager, compliant to ANSI /TIA 568.2-D CAT6A and ISO 11801 Class EA, with rear cable manager	
	Panel must be certified by Intertek labs for 4 connector channel performance for 15m short channel length and IEC 60603-7 plug performance. Certificates to be enclosed.	
	Shall be compliant and certified for IEEE 802.3bt 4PPoE transmission under 4 connector 100m channel.	
	The panel be intelligent ready to support AIM management functionalities as per ISO 18598, ANSI/TIA 5048 and ANSI/TIA 5017 when integrated with software.	
	Panel shall have plug retention force of 133N min.	
	Current Rating - 1.5 A @ 20 °C Dielectric Withstand Voltage, RMS - 1500 Vac @ 60 Hz Insulation Resistance, minimum - 500 MOhm	
	Material: high impact thermoplastic modules over powder coated steel frame	
	Shall be UL listed	
	Relative Humidity upto 95% non condensing.	

3. CAT6A UTP Patch Cord

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
Quantity	<ul style="list-style-type: none"> • Category 6A U/UTP Patch Cord 10 meters: 5450 • Category 6A U/UTP Patch Cord 12 meters: 1872 	
	Detail Functionalities	
	CAT6A U/UTP Patch Cord, solid construction, compliant to ANSI/TIA 568-CAT6A and IEEE 802.3bt 4PPoE.	
	LSZH sheath with UL 1863 listing.	
	Min Plug retention force: 133N or better	
	Patch cord shall be constructed with 24 AWG solid copper conductors with pair separator.	

	Patch Cords shall have maximum dc Resistance: 0.30 Ohm Safety voltage rating should be upto 300V.	
	Offered CAT6A Patch cord shall support intelligent cable detection mechanism and function when used with AIM system.	
	Certified for IEEE 802.3bt (4PPoE) transmission upto 60 Deg C under 4 connector 100m channel.	

4. CAT6A UTP modular (RJ-45) jacks

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	The CAT6A UTP 8-pin modular (RJ-45) jacks shall have Electrical performance guaranteed to meet or exceed the channel specifications of ISO/IEC 11801 Class EA and ANSI/TIA-568-C.2 Category 6A.	
	The information outlet shall support IEEE 802.3bt (Type 4) and have a Current Rating of 1.5 A at 20°C. Shall be compliant to IEC 60512-99-002 for safe unmating under electrical load.	
	Insulation Resistance, minimum: 500 MOhm	
	Shall have IEC 60603-7 certified plug performance. Intertek report to be enclosed.	
	Plug retention force, min: 133N	
	Shall support mating cycle durability under 4PPoE (90W) transmissions upto min 3000 mating cycles.	
	Faceplate shall be available with 1 or 2 port configuration.	
	Shall be UL 94V-0 rated.	

5, Work Area Faceplate

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	

	Faceplate shall be in 2 port square version, with shutter.	
	Faceplate Material shall be high impact, flame retardant, UL-rated 94 V-0, thermoplastic.	
	General Specifications a) Color: White b) Width: 86.36 mm (3.4 in) c) Height: 86.36 mm (3.4 in) d) Depth: 8.00 mm (0.31 in)	

6. MODULAR FIBER PANEL 1U, INTELLIGENT READY

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Modular type 1U fiber panel, shall accommodate (4) nos of MPO modules, for upto 48 duplex LC ports.	
	The sliding 1U panels shall have min 450mm depth for adequate storage space for trunk cables.	
	All Fiber panels shall have integrated front patch cord management trough and admin labeling window.	
	The fiber panel shall be intelligent ready to support AIM management functionalities as per ISO 18598, ANSI/TIA 5048 and ANSI/TIA 5017 when integrated with software.	
	Shall be made of powder coated steel with UL 94V-0 rating.	

7. Modular Fiber Panel 4U, Intelligent Ready

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Modular type 4U fiber panel enclosure, shall accommodate (24) nos of MPO modules, for upto	

	288 duplex LC ports.	
	The sliding 4U panel shall have min 500mm depth for adequate storage space for trunk cables.	
	Fiber panel shall have integrated front patch cord management trough and admin labeling window.	
	High density Panel shall support front slide-out option of only 2 tray elements/RU such that the other half of the tray is undisturbed. This is required to efficiently access high density fiber panel ports.	
	The fiber panel shall be intelligent ready to support AIM management functionalities as per ISO 18598, ANSI/TIA 5048 and ANSI/TIA 5017 when integrated with software.	
	Shall be made of powder coated steel with UL 94V-0 rating.	

8. PRE-TERMINATED MPO MODULES – MULTIMODE OM4, INTELLIGENT

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	MPO – LC 24F Cassette	
	The 24-fiber module shall have 12 pre-installed duplex LC adapters at the front routed to 2x12-fiber / 1x24-fiber Low loss OM4 MPO adapters at the back.	
	All MPO modules must support 'Method B' wiring pattern for ease of scalability. Same cassette should be used in both end of the link, without need of flipped or straight wiring management.	
	Dust caps on each port must be translucent to support VFL tests, without removing caps. Test light should be visible at the remote end, even with dust caps ON.	
	The cassettes shall be UL 1863 listed.	
	MPO Modules must be intelligent ready to support AIM functionalities.	
	Max Loss of a typical MPO 50m channel with 6 MPO connections shall not exceed 2.40dB. Documentary evidence to be provided.	
	Cabling OEM shall have their own ISO 9001 & 14001 manufacturing facility for design and development of LAN & WAN equipment.	

9. 2x12F MPO Trunk Cable, OM4

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
Quantity	<ul style="list-style-type: none"> • 2x12F MPO Trunk Cable, OM4 10 meters: 46 • 2x12F MPO Trunk Cable, OM4 12 meters: 60 • 2x12F MPO Trunk Cable, OM4 15 meters: 66 • 2x12F MPO Trunk Cable, OM4 18 meters: 76 • 2x12F MPO Trunk Cable, OM4 20 meters: 14 • 2x12F MPO Trunk Cable, OM4 22 meters: 18 • 2x12F MPO Trunk Cable, OM4 25 meters: 24 • 2x12F MPO Trunk Cable, OM4 30 meters: 4 	
	Detail Functionalities	
	Low Loss MPO-12/UPC to MPO-12/UPC, Pre-terminated, LSZH, 24F OM4 Trunk Cable compliant to ANSI/ICEA S-83-596, Telcordia GR-409, IEC 60794-1, IEC 60793-2-10, TIA 492AAAD (OM4).	
	MPO trunk cable shall be configured and available with 12F/24F/48F/96F trunk configurations as per design requirement.	
	The offered MPO solution must support the given list of applications and SAN links as per RFP performance specifications. MPO should follow Method B wiring methodology for simple design installation.	
	MPO connector shall have Max Insertion Loss of 0.27dB. Min Return loss of MPO shall be \geq 27dB.	
	Trunk cable shall support Tensile strength upto 650N.	
	All OM4 trunk cables must have Aqua colored jacket as per TIA and ISO standards recommendation. Any non-standard color other than Aqua is not acceptable.	
	Flame rating shall be NEC OFNR (ETL) suitable for data center installations. The cable must have the flame test compliance to IEC 60332-3, IEC 60754-2, IEC 61034-2, IEEE 383, UL 1666 and UL 1685	
	Cable must be EN50575 CPR rated as Dca or better.	

10. **LC – LC Multimode Duplex Fiber Patch Cord**

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
Quantity	<ul style="list-style-type: none"> • LC – LC Multimode Duplex Fiber Patch Cord 8 meters: 5330 • LC – LC Multimode Duplex Fiber Patch Cord 10 meters: 2770 	
	Detail Functionalities	
	LC/UPC to LC/UPC, Multimode OM4 duplex Fiber Patch Cord, 1.6mm duplex cordage, Aqua, compliant to ICEA-S-83-596 and Telcordia GR 409.	
	Low Smoke Zero Halogen (LSZH) compliant to IEC 60332-3, IEC 60754-2, IEC 61034-2, UL 1666, UL 1685	
	Shall be strengthen with aramid yarns. Tensile rating should be 170N or better.	
	Connector Optical Performance Insertion Loss, maximum: 0.25 dB Return Loss, minimum: 27.0 dB	

11. **Intelligent Upgrade Kit, Copper Panels**

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Upgrade kit for 24 port Copper panels, 1U, pack of 10.	
	Shall support retro-fit connection on panels without any disconnection. UL listed.	

11. Intelligent Upgrade Kit, Fiber Panels

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Upgrade kit for 96F / 48 duplex Fiber ports, pack of 5 or more.	
	Shall support retro-fit connection on panels without any disconnection. UL listed.	

12. Intelligent Rack Controller

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	The Intelligent System Controller should be 19" Rack Mountable	
	The Intelligent System Controller Should occupy no more than 1 U rack space with the capability for 0U mounting	
	The Intelligent System Controller Should be able to manage upto 45 nos of 1U Copper or Fiber Panels per rack (1080 ports)	
	Only one Intelligent System Controller shall be required per rack. System controller shall have the flexibility to extend beyond one rack, for managing limited number of panels in adjacent racks.	
	Should have color LCD Screen with a touch sensor interface to Display - status, complete Circuit trace, alarms and work order at rack level.	
	The Intelligent System Controller shall be equipped with an	

	LED indicator to enhance visual communication to the technician.	
	The Intelligent System Controller shall provide audible Alerts /Alarms to the technician while the technician is performing various MAC activities	
	The Intelligent System Controller shall be able to display live end-to-end tracing information on its LCD screen during patching activities.	
	The Intelligent System Controller LCD screen shall have ability to turn off the backlight when not in use.	
	The Intelligent System Controller shall be able to display tracing information on its LCD screen	
	The Intelligent System Controller shall be able to display on the LCD screen information indicating if a traced panel port is assigned to a scheduled work order.	
	Multiple Intelligent System Controllers shall be able to interconnect together using serial bus architecture such as “daisy chain”, with standard modular RJ45 patch cords.	
	The Intelligent System Controller shall have a configurable Ethernet LAN connection capability to enable communication with Intelligent Infrastructure Operations Software.	
	Enabling of Ethernet capabilities for a System Controller System shall be in built, without need for any external devices	
	Unlimited scalability of adding Ethernet enabled Intelligent Controllers on the network	
	The Intelligent System Controller should have Dual power supply for Power redundancy	
	The Intelligent System Controller shall provide the ability to configure local “patching zones”	
	The Intelligent System Controller shall support IPv6 communications	

13. Intelligent System Software, Per Port License

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Shall comply to ISO/IEC 18598 and ISO/IEC 14763-2 -- Automated infrastructure management (AIM) systems to	

RESTRICTED

	monitor upto min 5000 managed ports.	
	System shall have single tier distributed architecture (single controller vs. cascading/multi-tier controllers, single controller is capable to communicate to intelligent patch panels directly).	
	System shall require only three components for system design: intelligent patch panels, single system controller and software.	
	System shall provide full featured electronic work order capabilities that include: a) Guided MAC activities through the use of LED indicators at panel's ports b) Audible feedback to a technician to ensure accuracy of performed MAC activities c) Color LCD Screen with a touch screen interface to Display status, complete Circuit trace, alarms and work order.	
	System shall be capable to support cross-connect as well as interconnect administration topology.	
	Software shall feature split screen view showing all assets, rack view, circuit / connectivity views, asset details etc. in single screen.	
	System shall enable full-featured remote administration capabilities either via a software client or a web client that include electronic work orders, database access, etc.	
	System shall be able to generate real-time security alerts upon: a) Insertion of a plug into intelligent panel port b) Removal of a plug from intelligent panel port c) Pressing of a trace button above panel port d) Unauthorized MAC activity in telecom room	
	Software should be able to detect/report in real time any connection or disconnection made in the network using standard RJ45, LC and MPO patch cords.	
	The Software shall be capable of importing, displaying and printing CAD drawings for accurate representation of building's floor plans.	
	The Software shall have capability to auto discover the installed intelligent hardware (intelligent panels and control systems) in each rack/cabinet and to auto populate this information in its database.	
	The Software shall provide the capability to allow external Software systems (for example Aperture, Remedy HelpDesk, HP Service Manager, etc.) to interact with the AIM Solution.	
	AIM system shall be able to detect POE information with details like PoE Class, wattage of power being utilized and identification of cable bundles using POE.	
	AIM system shall be able to demarcate outside plant fiber conduits / fiber pits for route identification and capacity	

	planning.	
	Software shall be available with port based licensing and easy to scale as the network grows.	
	The Solution must support field upgrade of intelligence-ready passive copper and fiber panels without removal of existing patch cords and without disruption of network services. All non-intelligent panels should be upgradable to intelligent panels without any patch cord disconnection or removal.	

14. Fiber Guide Pathway System

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	The contractor should design the Complete fiber runner solution. The contractor must consider the necessary accessories like thread rod, bolt & nut, Supporting angle, fiber drop, bend, T joint, 4 way Junction, straight coupler.	
	The fiber raceways system shall be available in 4-, 6-, 12- and 24- inch dimensions.	
	Fiber runner and accessories shall have height of 4 inch at minimum, at all sections of the pathway.	
	All system components and joints must have modular snap-fit design, without the use of screw, nuts or bolts.	
	Each rack should have one fiber drop of adequate dimension. From fiber drop to rack top cable must pass through flexible hose.	
	Material Construction: <ul style="list-style-type: none"> ○ All materials in the offered overhead fiber routing systems must meet UL 94V-0 and Bellcore TR-EOP-000063 standards compliant. This excludes the flex tube drops. ○ System shall be made from a low-smoke, non-brominated, non-chlorinated, flame retardant material and is loaded stress tested under high temperature and humidity to verify durability under extreme conditions ○ All materials used in the systems must comply with NEC and NEBS standards for fire 	

	<p>resistance.</p> <ul style="list-style-type: none"> ○ The under floor / suspended ceiling system must meet grounding requirements as specified in section 300-10 of the National Electric Code (NEC). ○ No overhead system offered shall contain metal, nylon or poly-vinyl chloride (PVC) materials. 	
	Fiber pathway system shall be of the same OEM make as of the proposed fiber cabling.	
	Fiber patch cord bend radius of at least two inches (5.08 cm) shall be maintained at all points in the offered system.	
	<p>All sections including, but not limited to the following must be considered in the design:</p> <ul style="list-style-type: none"> - 6-foot horizontal straight section 4x6 - 4x6 90° horizontal elbow - 4x6 T-Bends - 4-inch Express Exit - 2-Inch Express Exit - 2x2 flex tube attachment - 12mm Threaded rod Bracket kit - End Caps - Snap fit junctions 	
	Each section shall be supplied with snap fit or hinged covers.	
	Fiber pathway system shall be of bright Yellow color, for ease of identification.	

15. Copper Wire Basket Pathway System

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Dimension: Copper Pathway 300mm x 100mm x 2000m (WxHxL)	
	<p>Features:</p> <ul style="list-style-type: none"> ○ Easy to install and aesthetically pleasing ○ Simple Grounding/Bonding methodology ○ Light weight compared to ladders ○ Ideal for data cabling requirements ○ EMI/EMC containment for high frequencies 	

	<ul style="list-style-type: none"> ○ Ensures cable lay is compliant to TIA-568C guidelines ○ Cables should be easily accessible in the basket and help for MAC's ○ Choice of multiple pieces to meets complex cabling lay patterns ○ Open mesh design supports easy airflow ○ Uniform rib/rod dia (5mm) to ensure the consistent load baring across all cross Sections ○ Material shall be Mild steel ○ Shall provide bend radius controlled drop down kits for cable drop into each rack 	
	The Pathway system shall provide 100mm (4inch) high side walls for sufficient cable placement.	
	Each 300mm x 100mm straight section shall be 2000mm long.	
	Shall be equipped with Horizontal -T Bends and Horizontal Elbow bends	
	System shall be suspended from the ceiling using M12 threaded rods, 1.8 mtr long.	
	Bend radius controlled drop kits must be supplied for cable drop in each rack.	

16. **Power Cabling**

- a. **Brand:** To be mentioned by bidder. (Preferably BRB)
- b. **Model:** To be mentioned by bidder
- c. **Country of Origin:** As per technical specification, article 20
- d. **Country of Manufacturer:** As per technical specification, article 20

17. **Overhead hanging cable tray for Network Cables**

- a. **Brand:** To be mentioned by bidder. (Preferably CommScope / Panduit)
- b. **Model:** To be mentioned by bidder
- c. **Country of Origin:** As per technical specification, article 20
- d. **Country of Manufacturer:** As per technical specification, article 20

18. **Fiber Cable Runner**

- b. **Brand:** To be mentioned by bidder. (Preferably CommScope / Panduit)
- b. **Model:** To be mentioned by bidder
- c. **Country of Origin:** As per technical specification, article 20
- d. **Country of Manufacturer:** As per technical specification, article 20

19. **Cable Laying Service**

RESTRICTED

Bidder must survey and quote for cable laying services. Any accessories needed apart from the mentioned item in Annex J & Annex L, bidder must provide at their own cost to complete the project.

TECHNICAL SPECIFICATION OF CABLING- FIBER AND UTP
UTP CABLING

Structured Cabling System for All UDC (Command HQ &Base)

1. CAT 6 UTP LSZH Cable: 305 Meter /box

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
Detail Functionalities	CAT6 UTP 23 AWG Solid Cable should meet and exceed ANSI/TIA 568.2-D Category 6 and ISO/IEC 11801 Class E Specifications	
	Cable shall be constructed with pair separator and have round cable design.	
	The nominal Outside diameter should not be more than 6.0mm	
	The weight of the cable box of 1000 Feet should not be less than 24.5 lb	
Electrical properties	Max DC Resistance: ≤ 7.61 Ohms/100m	
	Max. Operating voltage: 80 V	
	Mutual Capacitance: 5.6 nF/100m @1kHz	
Environmental & Safety features	Operating temperature of -20 to 60 °C	
	ROHS 2011/65/EU compliant	
	The cable shall have Low-Smoke, Zero Halogen (LSZH) jacketing and must comply with the following Fire Safety standards: 1) ISO/IEC 60332-3-22: Vertical Flame Spread 2) ISO/IEC 60754-2: Acidity 3) ISO/IEC 61034-2: Smoke Density	
	Cable shall be compliant to EN50575 CPR Cable EuroClass and certified for Dca, s2, d2, a1 standards. Certificate should be submitted with bid.	
Certifications and Test Reports	Category 6 cable alongwith offered channel components should be certified by Intertek lab under 4 connector channel configuration to the requirement of ANSI/TIA 568-C.2 for long channel (100m) as well as short links (<15m). Test Certificates to be provided with bid.	
	Cable shall be ETL verified as per ANSI/TIA 568-C.2 and ISO/IEC 11801 for CAT6 requirements.	

	Factory test reports for CAT6 cable must be available for verification of authenticity, at OEM website with unique print string on individual cable jacket.	
--	---	--

2. CAT6 Patch Panel 24 Port (1U)

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	CAT6 Patch Panel 24 port (1U) complaint to ANSI/TIA-568-D.2 and ISO/IEC 11801 Class E	
	Shall support IEEE 802.3bt (type 4) application	
	The panel shall be equipped with rear cable management with min 4 nos of cable bundle managers for 24 port	
	The panel shall be UL and cUL Listed	
	Plug retention strength 133N	
	Electrical performance:	
	Current Rating - 1.5 A @ 20 °C	
	Dielectric Withstand Voltage, RMS - 1500 Vac @ 60 Hz	
	Insulation Resistance, minimum - 500 MOhm	
	Operating temperature: -10 °C to +60 °C	
	Material: Powder coated steel, UL 94V-0 rated	

3. CAT6 UTP Modular (RJ-45) jacks

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	The CAT6 UTP 8-pin modular (RJ-45) jacks shall be certified by Intertek for performance to channel specifications of ISO/IEC 11801 Class E and ANSI/TIA-568.2-D Category 6.	
	Information outlet shall have IDC connector terminations	

	on rear of base allow quick and easy installation of 22 to 24 AWG cable	
	Each outlet shall be supplied with rear protective strain relief cap to protect against contamination and securing the termination.	
	Electrical properties:	
	The information outlet shall have a Current Rating of 1.5 A at 20°C	
	Insulation Resistance, minimum: 500 MOhm	
	Contact Resistance, maximum: 100 mOhm	
	Contact Resistance Variation, maximum: 20 mOhm	
	Dielectric Withstand Voltage, RMS, conductive surface: 1,500 Vac @ 60 Hz Dielectric Withstand Voltage, RMS, contact-to-contact : 1,000 Vac @ 60 Hz	
	Mechanical performance:	
	Material: High-impact, flame retardant, thermoplastic, UL 94V-0 rated	
	Shall be IEC 60603-7 compliant and IEC 60512-99-002 for safe unmating	
	Plug insertion life, Min: 3000 cycles under 90W PoE power.	
	Plug retention force, min: 133N	
	Should be UL and cUL listed	

4. CAT6 UTP Patch Cord

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
Quantity	<ul style="list-style-type: none"> • Category 6 UTP Patch Cord for User End 1 mete: 1500 • Category 6 UTP Patch Cord for User End 2 meters: 5000 • Category 6 UTP Patch Cord for User End 3 meters: 400 • Category 6 UTP Patch Cord for Patch Panel End: 700 	
	Detail Functionalities	
	CAT6 UTP Patch Cord, shall be of 4 pair stranded construction, with pair separator.	
	Offered CAT6 Patch cord shall support intelligent cable detection mechanism and function with the proposed AIM system.	

	Cords shall be factory terminated with 8-pin modular plugs on each end.	
	The cordage shall be UTP components that do not include internal or external shields, screened components or drain wires.	
	Patch Cord shall have LSZH jacket complying with the following Fire Safety standards: ISO/IEC 60332-1 ISO/IEC 60754-2: Acidity ISO/IEC 61034-2: Smoke Density	
	Min Plug retention force: 133N	
	Patch Cords shall have maximum dc Resistance:0.30 Ohm	
	Safety voltage rating: 300 V	
	Must be compliant with the channel specifications of ANSI/TIA 568-C.2. ROHS compliant and EN 50575 Dca compliant.	

5. CAT6A Modular Faceplate

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Shall be available in 2 port square version with shutters.	
	General Specifications a) Color: White b) Width: 86.36 mm (3.4 in) c) Height: 86.36 mm (3.4 in) d) Depth: 8.00 mm (0.31 in)	
	Material shall be high impact, flame retardant, UL-rated 94 V-0, thermoplastic.	

6. CAT6 F/UTP Double Jacketed Outdoor Cable for Ship & Jetty

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	

Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	CAT6 F/UTP Double Jacketed Outdoor Cable, 4 pair with cross filler separator, filled with water protective gel compound, compliant to ANSI/TIA 568.2-D and ISO/IEC 11801 Class E, suitable for outdoor and buried applications.	
	Shall be compliant to IEEE 802.3bt (Type 4) for 4PPoE transmissions.	
	Jacket Type: Outer: PE, UV protected Inner: PE Conductor: 23 AWG Solid Copper	
	Shield / Armor: Aluminium tape shielding between dual jackets. Drain wire: Shall have tinned copper drain wire Primary Insulation: Polyolefin / Polyethylene, Outer Sheath: UV protected, Black Nominal O.D.: Overall: 8.2 – 9.2 mm, Operating Temperature: -20 °C to 70°C	
	Conductor Resistance <=9.38 Ohms / 100 Meter Safety voltage rating – 300 V Di-electric strength, Min- 1500 Vac	
	Shall have water protective gel filling to prevent degradation due to moisture.	

7. CAT 6 F/UTP Outdoor Patch Cord for Jetty

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	CAT 6 F/UTP Outdoor Patch Cord compliant to ANSI/TIA 568-C.2, IEEE 802.3bt (type 4) and ROHS	
	Conductor: 24 AWG solid cordage	
	Min Plug retention force: 133N Plug Mating life: Min 750 cycles. Safety voltage rating: 300 V Max. DC Resistance: 0.30 Ohm	
	Contact plating material: Gold over Nickel underplate	
	ETL / CM-LS listed	

Operating temp range: -40 °C to +60 °C
--

FIBER OPTICS CABLING

Fiber Optic Components for all UDC (Command HQ & Base)

8. 6 CORES – Singlemode Outside Plant Fiber Cable

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	6 core Singlemode (OS2), Single Jacket, Corrugated steel tape armor, Gel-filled, Indoor/Outdoor Loose tube Fiber cable.	
	Compliance: ITU-T G.652.D (OS2), ITU-T G.657.A1 (bend insensitive).	
	Construction Materials: a) Jacket Material: LSZH b) Environmental space: Buried, Duct and Indoor/outdoor applications. c) Number of fibers per tube: 6 d) Subunit Type: 2.8mm buffer tube e) Jacket: LSZH as per IEC 60332-3-24	
	Mechanical Specifications: a) Cable Diameter: 8.00 - 10.00 mm b) Cable Weight: 80 – 100 kg/km c) Tensile Load, long term, Max: 800 N or better d) Tensile Load, short term, Max: 1500 N or better e) Operating Temperature: -40 degree Celsius to +70 degree Celsius	
	Mechanical Test Specifications a) Compression: 15 N/mm (as per IEC 60794-1 E3) b) Water Penetration Test Method: 24 h (as per IEC 60794-1 F5)	
	Optical Specifications Attenuation, Maximum a) 0.22 dB/km @ 1550 nm b) 0.36 dB/km @ 1310 nm	

10. 1U Fiber Rackmount Shelf, Sliding

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	1U Sliding Fiber Panel Shelf, accepts 4 nos of LC adapter packs or splice cassettes and splice trays, for a max of 48 fiber splices per unit.	
	The width shall be 19 inches, with a minimum of 18 inch depth.	
	The shelf/LIU shall have front sliding mechanism for better access to fiber connectors / couplers.	
	The Fiber shelf shall have integrated front patch cord trough	
	Shall be supplied with fiber management drums / rings and splice accessories	
	Min 6 cable inlet ports on rear of shelf.	

11. Rolo Splice Kit

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Splice Kit with 2 fusion splice trays	
	Compatible with above 1U Fiber shelf	
	Max splice capacity upto 32 fibers	

12. 12F LC SM Splice Cassettes

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	

Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Factory fitted fiber cassette assembly pre-installed with 6 duplex LC SM adapters and 12xLC SM pigtails	
	Pigtail shall be 900 micron tight buffered SM as per G.652.D and G.657.A1, OS2	
	Pigtails on each port shall be individually color coded as per TIA 598 for easy identification	
	LC ports should be supplied with external dust covers.	
	Insertion loss: 0.30dB or less	
	Return Loss: 55 dB or higher	
	UL listed	

13. 6F SM LIU FULLY LOADED, 1U

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	Shall be fully loaded and factory fitted with 6 LC duplex adapters, 12x LC SM Pigtails, splice trays, and fiber management rings	
	19" rack mountable 1U sliding shelf enclosure for secured splicing and patching.	
	Material powder coated steel for rugged finish.	
	Min 4 cable entry points at rear of shelf. Min 320mm depth for slack storage inside shelf.	
	Pigtail shall be constructed of SM G.657A1 fiber with LC/UPC end face	
	Individually color coded pigtails as per TIA 598 color code.	
	Insertion Loss, max: ≤ 0.25 dB Return Loss, min: >50 dB.	

14. LC – LC Singlemode Duplex Fiber Patch Cord 3 meters

Feature List	Feature Description	Bidders Response
Brand	To be mentioned by bidder. (Preferably CommScope / Panduit)	
Model	To be mentioned by bidder	
Country of Origin	As per technical specification, article 20	
Country of Manufacturer	As per technical specification, article 20	
Model / Part Code	Bidder to mention	
	Detail Functionalities	
	LC/UPC to LC/UPC, Singlemode OS2 duplex 1.6mm Fiber Patch cords, compliant to ICEA-S-83-596 and Telcordia GR 409.	
	Patch cords shall be bend insensitive as per G.657A1 specifications.	
	Low Smoke Zero Halogen (LSZH) compliant to IEC 60332-3, IEC 60754-2, IEC 61034-2, UL 1666, UL 1685	
	Jacket Color: Yellow	
	Cord Protection: Aramid Yarns	
	Supported tensile load upto 170N or better	
	Connector Optical Performance Insertion Loss, maximum: 0.30 dB Return Loss, minimum: 50.0 dB	
	Shall be NEC OFNR (ETL) Listed.	
	Shall be EN 50575 and ROHS compliant.	

15. Cable Laying Service (Qty: As Required)

Bidder must survey and quote for cable laying services. Any accessories needed apart from the mentioned item in Annex J & Annex L, bidder must provide at their own cost to complete the project.

TECHNICAL SPECIFICATION OF DATA LINK- NTTN

Name of the ISP 1: To be mentioned
 Name of the ISP 2: To be mentioned

Ser	Source	Destination	Path	Port Speed	Bandwidth	ISP	NTTN	One Time Cost	Monthly Recurring Cost
1.	CDC	NHQDC	Primary	2 x 10G 2 x 8G 2 x 10G 2 x 1G	1GB 4GB 4GB 100 MB				
2.	CDC	NHQDC	Secondary	2 x 10G 2 x 8G 2 x 10G 2 x 1G	1GB 4GB 4GB 100 MB				
3.	CDC	DRDC	Primary	1 x 10G 1 x 8G 1 x 10G 1 x 1G	1GB 4GB 4GB 100 MB				
4.	CDC	DRDC	Secondary	1 x 10G 1 x 8G 1 x 10G 1 x 1G	1GB 4GB 4GB 100 MB				
5.	NHQDC	DRDC	Primary	1 x 10G 1 x 8G 1 x 10G 1 x 1G	1GB 4GB 4GB 100 MB				
6.	NHQDC	DRDC	Secondary	1 x 10G 1 x 8G 1 x 10G 1 x 1G	1GB 4GB 4GB 100 MB				
7.	CDC	COMDHAKA (+BNS HAJI MOHSIN) at Dhaka.		1 x 10G	20 MB				
8.	CDC	COMCHIT (+ provision to link to FB) at Chattogram.		1 x 10G	20 MB				
9.	CDC	CSD(+CNRD +IFF Center) at Chattogram		1 x 10G	20 MB				
10.	CDC	COMBAN (+OSTG) at Chattogram.		1 x 10G	20 MB				
11.	CDC	COMNAV (+NAVAL AVIATION HANGAR) at Chattogram.		1 x 10G	20 MB				
12.	CDC	COMSUB (+ SUBMARINE BASE PAKUA) at Pakua		1 x 10G	20 MB				
13.	CDC	COMSWADS (+BNS NIRVIK) at Chattogram		1 x 10G	20 MB				

RESTRICTED

Ser	Source	Destination	Path	Port Speed	Bandwidth	ISP	NTTN	One Time Cost	Monthly Recurring Cost
14.	CDC	CHIEF HYDROGRAPHER (+BNHOC + NAI0) at Chattogram		1 x 10G	20 MB				
15.	CDC	COMKHUL (+BNS TITUMIR+BNS UPSHAM+ provision to Link to FB) at Khulna.		1 x 10G	20 MB				
16.	CDC	COMFLOT WEST (+BNS MONGLA+ BN D/Y MONGLA) at Mongla.		1 x 10G	20 MB				
17.	CDC	Commandant NATDOC (+BNS SHERE-E-BANGLA) at Patuakhali.		1 x 10G	20 MB				
18.	CDC	BNS SHEIKH MUJIB at Dhaka.		1 x 10G	20 MB				
19.	CDC	RIP MIRPUR at Dhaka		1 x 10G	20 MB				
20.	CDC	NAVY HOUSE at Dhaka		1 x 10G	20 MB				
21.	CDC	NU PAGLA at Dhaka		1 x 10G	20 MB				
22.	CDC	BNS ISSA KHAN at Chattogram.		1 x 10G	20 MB				
23.	CDC	BNS ULKA at Chattogram.		1 x 10G	20 MB				
24.	CDC	BNS SHAHEED MOAZZAM at Kaptai.		1 x 10G	20 MB				
25.	CDC	BNS BHATIARY at Chattogram.		1 x 10G	20 MB				
26.	CDC	BNA at Chattogram.		1 x 10G	20 MB				
27.	CDC	SMWT at Chattogram.		1 x 10G	20 MB				
28.	CDC	BNS PATENGA at Chattogram.		1 x 10G	20 MB				
29.	CDC	RIP Chattogram (Sailor's Colony 2).		1 x 10G	20 MB				
30.	CDC	SO/BSO Ctg at Chattogram.		1 x 10G	20 MB				

RESTRICTED

Ser	Source	Destination	Path	Port Speed	Bandwidth	ISP	NTTN	One Time Cost	Monthly Recurring Cost
31.	CDC	BN RRB at Chattogram.		1 x 10G	20 MB				
32.	CDC	Fwd Base Cox's Bazar		1 x 10G	20 MB				
33.	CDC	RIP Khulna		1 x 10G	20 MB				
34.	CDC	BNS SOLAM at Khulna		1 x 10G	20 MB				
35.	DRDC	COMDHAKA (+BNS HAJI MOHSIN) at Dhaka.		1 x 10G	20 MB				
36.	DRDC	COMCHIT (+ provision to link to FB) at Chattogram.		1 x 10G	20 MB				
37.	DRDC	CSD (+CNRD+IFF Center) at Chattogram.		1 x 10G	20 MB				
38.	DRDC	COMBAN (+OSTG) at Chattogram.		1 x 10G	20 MB				
39.	DRDC	COMNAV (+NAVAL AVIATION HANGAR) at Chattogram.		1 x 10G	20 MB				
40.	DRDC	COMSUB (+SUBMARINE BASE PAKUA) at Pakua.		1 x 10G	20 MB				
41.	DRDC	COMSWADS (+BNS NIRVIK) at Chattogram		1 x 10G	20 MB				
42.	DRDC	CHIEF HYDROGRAPHER (+BNHOC + NAIO) at Chattogram		1 x 10G	20 MB				
43.	DRDC	COMKHUL (+BNS TITUMIR+BNS UPSHAM+ provision to Link to FB) at Khulna.		1 x 10G	20 MB				
44.	DRDC	COMFLOT WEST (+BNS MONGLA+ BN D/Y MONGLA) at Mongla.		1 x 10G	20 MB				
45.	DRDC	Commandant NATDOC (+BNS SHERE-E-BANGLA) at Patuakhali.		1 x 10G	20 MB				

RESTRICTED

Ser	Source	Destination	Path	Port Speed	Bandwidth	ISP	NTTN	One Time Cost	Monthly Recurring Cost
46.	DRDC	BNS SHEIKH MUJIB at Dhaka.		1 x 10G	20 MB				
47.	DRDC	RIP MIRPUR at Dhaka		1 x 10G	20 MB				
48.	DRDC	NAVY HOUSE at Dhaka		1 x 10G	20 MB				
49.	DRDC	NU PAGLA at Dhaka		1 x 10G	20 MB				
50.	DRDC	BNS ISSA KHAN at Chattogram.		1 x 10G	20 MB				
51.	DRDC	BNS ULKA at Chattogram.		1 x 10G	20 MB				
52.	DRDC	BNS SHAHEED MOAZZAM at Kaptai.		1 x 10G	20 MB				
53.	DRDC	BNS BHATIARY at Chattogram.		1 x 10G	20 MB				
54.	DRDC	BNA at Chattogram.		1 x 10G	20 MB				
55.	DRDC	SMWT at Chattogram.		1 x 10G	20 MB				
56.	DRDC	BNS PATENGA at Chattogram.		1 x 10G	20 MB				
57.	DRDC	RIP Chattogram (Sailor's Colony 2).		1 x 10G	20 MB				
58.	DRDC	SO/BSD Ctg at Chattogram.		1 x 10G	20 MB				
59.	DRDC	BN RRB at Chattogram.		1 x 10G	20 MB				
60.	DRDC	Fwd Base Cox's Bazar		1 x 10G	20 MB				
61.	DRDC	RIP Khulna		1 x 10G	20 MB				
62.	DRDC	BNS SOLAM at Khulna		1 x 10G	20 MB				
63.	DRDC	COMDHAKA (+BNS HAJI MOHSIN) at Dhaka.		1 x 10G	20 MB				
64.	DRDC	COMCHIT (+ provision to link to FB) at Chattogram.		1 x 10G	20 MB				
65.	DRDC	CSD (+CNRD+IFF Center) at Chattogram.		1 x 10G	20 MB				

TECHNICAL SPECIFICATION OF TOOLS & TEST EQUIPMENTTEST EQUIPMENT

Equipment Name	Description	Qty
SimpliFiber® Pro Optical Power Meter and Fiber Test Kits	<p>Complete Fiber Verification Kit (FTK1475):</p> <p>The Complete Fiber Verification Kit is for contractors and network technicians who install and maintain premises networks with both multimode and single mode optical fiber. Use this kit to verify optical loss and power levels at 850, 1300, 1310, and 1550 nm, inspect fiber end-faces, locate cable faults, connector problems, and polarity issues. Kit includes FI-500 Fiber Inspector Micro.</p>	02 Sets
MultiFiber™ Pro Optical Power Meter and Fiber Test Kits	<p>MFTK-SM1310-SM1550</p> <p>Multi Fiber Pro Single mode test kit includes Multi Fiber Pro Power Meter, 1310 nm laser light source, 1550 nm laser light source, Single mode test cords (1 unpinned/unpinned; 1 unpinned/pinned; 2 pinned/pinned), 2 APC MPO adapters, Magnetic strap attachments and carrying case.</p> <p>MFTK-MM850-SM1310</p> <p>MultiFiber Pro Multimode & 1310 nm Singlemode Kit includes MultiFiber Pro Power Meter, 850 nm Light Source, 1310 nm Light Source, Test Reference Cords, MPO adapters, Magnetic strap attachments and carrying case.</p>	
OptiFiber® Pro OTDR	<ul style="list-style-type: none"> • Multiple wavelengths (850, 1300, 1310,1490, 1550 and 1625 nm) support LAN, datacenters, PON, FTTx and outside plant applications. • Automated setup senses fiber characteristics and sets measurement parameters • Manual Expert mode allows simple adjustments to automated settings for detailed testing. • EventMap automatically identifies events including connectors, splices, bends, and splitters • Gesture-based interface allows fast, in-depth trace analysis • SmartLoop™ OTDR technology tests two fibers in a single test eliminating the need to travel to the far end of the connection to perform tests. 	

RESTRICTED

	<ul style="list-style-type: none"> • Instantaneous on-board bi-directional averaging results included as standard • Integrates with LinkWare™ Live to manage jobs and testers from any smart device. • Future-ready Versiv™ design supports copper certification to Category 8, fiber loss and inspection. 	
<p>LinkIQ Cable + Network Tester</p>	<ul style="list-style-type: none"> • Measure network cabling performance up to 10 Gig via frequency-based measurements • Troubleshoot active networks by providing connected switch information (Switch Name, IP Address, MAC Address, Port Number, and VLAN info) • Test connectivity to TCP/IP network through IP configuration and ping • Verify Gateway and DNS server responsiveness and availability 	
<p>Fiber Optic Cleaning Kits</p>	<ul style="list-style-type: none"> • Each fiber cable cleaner kit includes the supplies you need to eliminate the #1 cause of fiber optic link failure: contamination • Cleans all fiber connector types in datacenter and campus environments • Quick Clean™ Cleaners—no training required • Solvent pen precisely dispenses specially formulated fiber optic cleaning solution • Optical Fiber Cable (OFC) cleaner cards for convenient cleaning of fiber end-faces • Rugged NFC kit case stores and transports all fiber optic cleaning tools and supplies 	

TOOLS

Equipment Name	Description	Qty
Visual Fault Locator (VFL)	This handy tool should injects a visible red laser light into the fiber. If there's a crack or break, the light should leak out, making it easy to pinpoint the problem area.	
NAVITEK NT – NETWORK CABLE TESTER	<ul style="list-style-type: none"> • Network troubleshooting – pinpoint and solve network connectivity issues quickly • Network service detection – port info, IP/MAC addresses and operates on VLAN • Monitor network traffic – real time display of broadcast network traffic • Copper and fibre cable tests – wiremap, distance to fault, PoE, optical power indication • Professional PDF reports – send them from the site using the free TREND AnyWARE app 	02 sets
Pro'sKit® UTP/STP Cable Stripper	Brand: To be mentioned Model: To be mentioned Feature: 32 to 23AWG Stripping Punch Down	
Network Installation Tool Kit	Brand: To be mentioned Model: To be mentioned	
Network Repair Tools with tool box	Brand: To be mentioned Model: To be mentioned	
Hammer, Wrench and Drivers Tools with tool box	Brand: To be mentioned Model: To be mentioned	
BOM	Have to be provided	
Warranty	Three (03) years full	

Foreign Training Package

Training Category	Training Module	Category of Personnel	Content	Group	Training Premises & Duration
1. Intermediate IT Training – Project Management	Project Management Professional (PMP)	8 X Officer	a) Scope Management b) Time Management c) Cost Management d) Risk Management e) Professional Responsibility and Ethics	Group-1	Malaysia (02 weeks)
2. Intermediate IT Training – Facilities Operations	Certified Data Centre Facilities Operations Specialist (CDFOS)	5 X Officer 5 X Sailor	a) Introduction to Data Centre b) Centre Operations c) Data Centre d) Infrastructure Management e) Data Centre Security and Risk Management f) Maintenance and Disaster Recovery	Group 2 5 x Officer & 5 x Sailor will undergo CDFOS and CDFOM training.	Malaysia/ Thailand (05 Days)
	Certified Data Center Facilities Operations Manager (CDFOM)	5 X Officer 5 X Sailor	a) Data Center Infrastructure and Design b) Data Center Operations and Management c) Environmental and Energy Efficiency in Data Centers d) Data Centers Risk Management, Security and Compliance in Data Centers		Malaysia/ Thailand (05 Days)
3. Advanced IT Training – IT Management	ITIL4 Foundation	6 X Officer	a) Introduction to ITIL4 and its importance in networking b) Service Management and its relation to networking c) Key ITIL4 concepts for network management d) ITIL4 practices for network operations	Group 3 (6 x Officer will undergo this training 7 days training package)	Malaysia/ Thailand (03 days)
	ITIL 4 Specialist	6 X Officer	a) Design and implementation of IT services. b) Ensuring service quality, efficiency, and reliability. c) Agile and DevOps		Malaysia/ Thailand (04 days)

RESTRICTED

Training Category	Training Module	Category of Personnel	Content	Group	Training Premises & Duration
			principles in service delivery. d) IT service performance management and monitoring. □ Supporting continual improvement and innovation.		
4. Cyber Security Training	Certified Information Systems Security Professional (CISSP) (Optional)	6 X Officer	a) Security and Risk Management b) Asset Security c) Security Architecture and Engineering d) Communication and Network Security e) Identity and Access Management (IAM)	Group -4 6 x Officer will undergo total 2 weeks training package	Malaysia/ Singapore (10 Days)
	Certified Information Systems Auditor (CISA) (Optional)	6 X Officer	a) Information System Auditing Process b) Governance and Management of IT c) Information Systems Acquisition, Development, and Implementation d) Information Systems Operations and Business Resilience e) Protection of Information Assets	Group- 5 6 x Officer will undergo total 3 weeks training package	Malaysia/ Singapore (5 days)
	Certified Ethical Hacker (CEH)	6 X Officer	a) Introduction to Ethical Hacking b) Footprinting and Reconnaissance c) Network Scanning and Enumeration d) System Hacking and Malware Threats e) Web Application and Wireless Network Hacking		Malaysia (2 weeks)

RESTRICTED

Local Training Package

Training Category	Training Module	Content	Category of Personnel	Training Premises & Duration
1. Basic IT Training – Technical Support Specialist	Data Centre Operational Support Training	a) Introduction to Data Centre Operations b) Infrastructure Management and Monitoring c) Network and Security Management d) Data Backup and Disaster Recovery e) Performance Optimization and Troubleshooting	5 X Officer 15 X Sailor	Bangladesh (05 Days)
	Cisco Certified Network Associate (CCNA)	a) Introduction to Networking b) IP Addressing and Subnetting c) Network Devices and Their Functions d) LAN Technologies and Ethernet e) Cisco Router and Switch Configuration f) Routing Protocols (RIP, OSPF, EIGRP) g) VLANs and Inter-VLAN Routing h) TCP/IP and OSI Model i) Network Security Fundamentals j) WAN Technologies and VPNs k) Network Troubleshooting and Tools l) IPv6 Addressing and Configuration	10 X Officer 10 X Sailor	Bangladesh (4 weeks)
2. Intermediate IT Training – System Administrator	Microsoft Certified-Server Administrator	a) Windows Server Installation and Configuration b) Active Directory Management and Group Policy c) Storage and File Systems Management d) Server Virtualization and Cloud Integration e) Network Infrastructure and Security Management	5 X Officer 5 X Sailor	Bangladesh (2-3 weeks)
	Red Hat Certified-Server Administrator	a) System Configuration and Management b) User and Group Management c) Filesystem and Storage Management d) Networking Configuration and Troubleshooting e) System Monitoring and Performance Optimization	5 X Officer 5 X Sailor	Bangladesh (2-3 weeks)
	Hyperconverge operational	a) Introduction to Hyperconvergence	5 X Officer 5 X Sailor	Bangladesh (5 days)

RESTRICTED

Training Category	Training Module	Content	Category of Personnel	Training Premises & Duration
	Training	b) Architecture and Components of Hyperconverged Infrastructure (HCI) c) Deployment and Configuration of Hyperconverged Systems d) Operational Management and Monitoring of HCI e) Troubleshooting and Optimization in Hyperconverged Environments		
3. Advanced IT Training – Network System Administrator	Cisco Certified Network Professional (CCNP) Data Center	a) Network Design and Architecture b) Advanced Routing Protocols c) Switching and Routing Troubleshooting d) Wireless Networking and Security e) Firewall Technologies and Configuration	4 X Officer 1 X Sailor	Bangladesh (2 months)
	Cisco Certified Network Professional (CCNP) Enterprise	a) Network Security Concepts and Technologies b) Secure Access Solutions (Identity Services Engine, 802.1X) c) VPN Technologies and Implementation d) Firewall Technologies and Configuration e) Intrusion Prevention and Detection Systems		Bangladesh (2 months)
4. Advance IT Training – Network Security Analyst	Cisco Certified Network Professional (CCNP) Security	a) Advanced Routing Protocols b) Layer 2 Technologies and Switching c) Network Security and VPNs d) Troubleshooting and Network Performance Optimization e) Wireless and QoS Implementation	5 X Officer	Bangladesh (2 months)

BILL OF QUANTITY

The bidder is to submit the Bill of quantity (without mentioning Unit price and Total price) in technical offer and complete bill of quantity (with price details) in financial offer.

COST FOR ACTIVE HARDWARE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
CDC (Active Equipment for Data Center)							
1.	Rack Server	15	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Hyperconverged Server (4 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Core Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Internet / DMZ Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	WAN Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	WAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Distribution Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	FC / SAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Spine Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Leaf Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	SDN Controller (3 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	DC-DR Replicator Switch (IPN)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Out of Band Management Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Multi Site Orchestration System (2 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	Core Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	WAN Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

17.	DMZ Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	Core Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	WAN Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	DMZ Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security (2 for Core & 2 for DMZ)	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Application Delivery Controller (ADC), Web Application Firewall & API Security	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
23.	Storage	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
24.	Back Up Storage	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
25.	Network Access Control	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
26.	WEB Security Appliance (WSA) 500 user	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
27.	Network Detection and Response (NDR)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
28.	Deep Discovery Inspection (DDI)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
29.	Anti-APT Solution (Sandbox)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
30.	IP telephony (Set)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Sub-Total (CDC (Active Equipment for Data Center)) =							To be mentioned
DRDC (Active Equipment for Data Centre)							
1.	Rack Server	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Hyperconverged Server (4 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Core Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

4.	Internet / DMZ Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	WAN Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	WAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Distribution Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	FC / SAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Spine Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Border Leaf Switch	0	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Leaf Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	SDN Controller (3 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	DC-DR Replicator Switch (IPN)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Out of Band Management Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	Multi Site Orchestration System (2 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	Core Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	WAN Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	DMZ Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	Core Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	WAN Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	DMZ Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
23.	Application Delivery Controller (ADC), Web Application	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	Firewall & API Security						
24.	Storage	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
25.	Back Up Storage Server	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
26.	Network Access Control	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
27.	Anti-APT Solution (Sandbox)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
28.	Network Detection and Response (NDR)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
29.	Deep Discovery Inspection (DDI)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Sub-Total (DRDC (Active Equipment for Data Centre)) =							To be mentioned
NHQ DC (Active Equipment for Data Center)							
1.	Rack Server	5	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Hyperconverged Server (4 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Core Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Internet / DMZ Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	WAN Router	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	WAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Distribution Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	FC / SAN Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Spine Switch	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Border Leaf Switch	0	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Leaf Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	SDN Controller (3 Node)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	DC-DR Replicator Switch (IPN)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Out of Band Management Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

15.	Core Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	WAN Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	DMZ Firewall	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	Core Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	WAN Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	DMZ Firewall 2	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Application Delivery Controller (ADC), Web Application Firewall & API Security	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
23.	Storage	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Sub-Total (NHQ DC (Active Equipment for Data Center)) =

UDC-COMDHQ & UDC-BASE (Active Equipment for Data Center/Network Room of Command HQ & Base)

1.	Rack Server for UDC	28	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Branch Router Type 1	28	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Branch Firewall 1 (200+ Users)	8	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Branch Firewall 2 (<50 & >200 Users)	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Branch Firewall 3 (>=50 Users)	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Distribution Switch	28	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	POE LAN Switch (L2)	400	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	Industrial Grade Ethernet switch (Jetty)	17	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Sub-Total (UDC (Active Equipment for Data Center)) =

UDC-SHIP (Active Equipment for Network Room)

1.	Branch Router Type 2	15	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
----	----------------------	----	-----------------	-----------------	-----------------	-----------------	-----------------

RESTRICTED

2.	Industrial Grade Firewall	15	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	POE LAN Switch (L2)	30	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Sub-Total (UDC-SHIP (Active Equipment for Network Room)) =							
Workstation PC (End User)							
1.	All in One PC	550	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Workstation for NOC and SOC	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Sub-Total (Workstation PC (End User)) =							
Printer & Scanner							
1.	Laser Printer (Colour- A4 , All in one)	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Laser Printer (Colour- A3)	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Laser Printer (Black and White)	05	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Scanner	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Sub-Total (Printer & Scanner) =							
Ancillary Equipment (CDC, DRDC, NHQ DC, Base & Ship)							
1.	Ancillary Item	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub- total of Active Hardware (CDC, DRDC, NHQ DC, Base & Ship) =							

COST FOR SOFTWARE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Software for CDC, DRDC, NHQ DC, UDCs, NOC, SOC, Management and End User PC)							
1.	Server OS License (Windows 2025 Standard Edition, Perpetual License)	80	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Server OS License (Windows 2025)	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	Enterprise Edition, Perpetual License)						
3.	Server Client Access License (CAL) (Subscription: 1 year)	550	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Server OS License (Linux) (Subscription: 1 year)	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Multi Factor Authentication (MFA) (Subscription: 3 years)	500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Email Security Gateway (Subscription: 3 years)	500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Extended Detection and Response (XDR) (Subscription: 3 years)	500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	SIEM & SOAR (Subscription: 3 years)	500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Privileged Access Management (PAM) (Subscription: 3 years)	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Active Directory Controller Software (To be included in Server OS)	500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Monitoring Software (Subscription: 3 years)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	Vulnerability Management Software (Subscription: 3 years)	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13	Active Directory (AD) Security	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	(Subscription: 3 years)						
14.	Penetration Testing Solution	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(Subscription: 3 years)						
15.	Server Security Solution (Subscription: 1 years)	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	DNS Firewall with DHCP and IPAM	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(Subscription: 3 years)						
17.	Windows OS for End User PC	530	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(To be included with PC)						
	(BitLocker to be included with the license)						
18.	Linux OS for NOC and SOC	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	End User- End Point Protection	570	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(Subscription: 1 years)						
20.	LB/WAF/DDos Management Software	3	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(Subscription: 3 years)						
21.	Backup Software	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
	(Subscription: 3 years)						
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Software (CDC, DRDC, NOC, SOC, Management and End User PC)) =							

COST FOR PASSIVE EQUIPMENT

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Passive Hardware for CDC							
Rack for Active Devices							
1.	Server Rack with KVM	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Rack without KVM	16	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Hot-aisle Containment System	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Power Arrangement							
1.	Automatic Voltage Regulator-800KVA	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Backup Online UPS Stand Alone-250KVA/KW	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Modular Online UPS-200KVA/KW (N+2 Modules)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	40KW Online UPS	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Isolation Transformer 250KVA	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Floor Mounted Power Distribution System-200A with Auto transfer Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Floor Mounted Power Distribution System-100A with Auto transfer Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	IT Power Distribution Module 3x1 Pole 3 Wire 32A	160	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	IT Power Distribution Module 3 Pole 5 Wire 32A	8	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	IT Power Distribution Module 3 Pole 5 Wire 63A (4 Units)	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Rack Automatic Transfer Switch for	15	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	single corded equipment						
12.	Transient Voltage Surge Suppression (TVSS)	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Signal reference grid system	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Data Center Earthing & Bonding system	06	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	Data Center Information Management system with Environmental management system BMS	01	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	Controlled electric lighting system (Electric lighting - Intelligent Lighting System))	01	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	Electrical Works	01	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	Power Cable Ladder	01	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	Electrical Switch Sockets	01	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Air Conditioning System

1.	Precision Air Conditioner (PAC)_DX for Server Room	02 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Precision Air Conditioner (PAC)_DX for MMR & Power Room	04 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Chiller	02 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Chilled Water (CW) Air Handling Unit for Server Room	02 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Chilled Water (CW) Air Handling Unit for MMR & Power Room	04 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Comfort Cooling (VRF for SOC, NOC, Staging room & Office area with corridor	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Fire Fighting System

1.	Very early smoke detection aspirating system (VESDA)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
----	--	---	-----------------	-----------------	-----------------	-----------------	-----------------

RESTRICTED

2.	Automated Fire Suppression system (GFSS)	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Fire Hydrant System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Portable Fire Extinguisher ABC Dry Power	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Portable Fire Extinguisher CO2	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Access Control System							
1.	Access Control with visitor management System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Baggage scanner	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Turnstile Gate with RFID Access control Module	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Walk through gate	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
CCTV System							
1.	Camera	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Network Video Recorder (NVR)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	LED TV	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Other System/ Equipment							
1.	Raised Floor	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Floor Insulation	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Dry wall & Paint	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Water leak detection system (WDS)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Lightning Protection System.	02 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Rodent System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	NOC with Gallery Type Seating Arrangement	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	SOC with Seating Arrangement.	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Fork-Lift for Equipment Movement.	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	PA System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

11.	Wireless Powered Desktop Laminated Label Printer	02	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	Dual Sided Card Printer with Ribbons & Cards.	02	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Fire Rated Door for Data Center	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Gensets & Substation							
1.	Express Line Feeder with RMU & HT Metering panel	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	11KV Isolator with vacuum contactor	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	HT Automatic Voltage Regulator (AVR) with Bypass Arrangement	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	11 KV H.T. Switchgear (VCB)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Cast Resin Dry Type Transformer	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Phase Correction Device (PCD)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	LT Switchgear	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	480 KVAR AUTOMATIC PFI PLANT	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	LIGHTNING ARRESTOR	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	ATS Panel, 1250A.	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	BUS BAR TRUNKING SYSTEM(BBT)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	CABLES AND CONNECTIVITY	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Earthing for Substation & Generator	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	FIRE FIGHTING SYSTEM FOR SUB STATION	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	FIRE FIGHTING SYSTEM for Generator Room	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	Power system monitoring (SCADA)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	Infrastructure Development Work for Substation and Generator Room	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

18.	Lightning Protection System.	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	MISCELLANEOUS	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	350KVA, GENERATOR	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	Day tank for Fuel of Generator	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Auto Fuel Refil System	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Underground Fuel Reservoir Tank	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
23	Ancillary Equipment.	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Passive Equipment for CDC) =							
Passive Hardware for DRDC							
Rack for Active Devices							
1.	Server Rack with KVM	11	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Rack without KVM	13	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Hot-aisle Containment System	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Power Arrangement							
1.	Automatic Voltage Regulator-500KVA	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Modular Online UPS-150KVA/KW (N+2 Modules)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Isolation Transformer 200KVA	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Floor Mounted Power Distribution System-100A with Auto transfer Switch	6	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Floor Mounted Power Distribution System-50A with Auto transfer Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	IT Power Distribution Module 3x1 Pole 3 Wire 32A	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

7.	IT Power Distribution Module 3 Pole 5 Wire 32A	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	IT Power Distribution Module 3 Pole 5 Wire 63A (4 Units)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Rack Automatic Transfer Switch for single corded equipment	12	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Transient Voltage Surge Suppression (TVSS)	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Signal reference grid system	03 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	Data Center Earthing & Bonding system	06 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Data Center Information Management system with Environmental management system BMS	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Controlled electric lighting system (Electric lighting - Intelligent Lighting System))	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	Electrical Works	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	Power Cable Ladder	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	Electrical Switch Sockets	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Air Conditioning System

1.	Precision Air Conditioner (PAC)_DX for Server Room	02 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Precision Air Conditioner (PAC)_DX for MMR & Power Room	08 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Chiller	02 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Chilled Water (CW) Air Handling Unit for Server Room	02 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Fire Fighting System

1.	Very early smoke detection aspirating system (VESDA)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
----	--	--------	-----------------	-----------------	-----------------	-----------------	-----------------

RESTRICTED

2.	Automated Fire Suppression system (GFSS)	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Portable Fire Extinguisher ABC Dry Power	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Portable Fire Extinguisher CO2	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Access Control System

1.	Access Control with visitor management System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Turnstile Gate with RFID Access control Module	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Walk through gate	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

CCTV System

1.	Camera	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Network Video Recorder (NVR)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	LED TV	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

Other System/ Equipment

1.	Raised Floor	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	DC Floor Insulation	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Dry wall & Paint	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Water leak detection system (WDS)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Lightning Protection System.	02 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Rodent System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	NOC with Gallery Type Seating Arrangement	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	Fork-Lift for Equipment Movement.	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	PA System	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Wireless Powered Desktop Laminated Label Printer	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Dual Sided Card Printer with Ribbons & Cards.	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

12.	Fire Rated Door for Data Center	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Gensets & Substation							
1.	Express Line Feeder with RMU & HT Metering panel	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	11KV Isolator with vacuum contactor	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	HT Automatic Voltage Regulator (AVR) with Bypass Arrangement	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	11 KV H.T. Switchgear (VCB)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Cast Resin Dry Type Transformer	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Phase Correction Device (PCD)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	LT Switchgear	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	300 KVAR AUTOMATIC PFI PLANT	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	LIGHTNING ARRESTOR	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	ATS Panel, 1250A.	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	CABLES AND CONNECTIVITY	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Earthing & Bonding	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	FIRE FIGHTING SYSTEM FOR SUB STATION	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	FIRE FIGHTING SYSTEM for Generator Room	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	Power system monitoring (SCADA)	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	Infrastructure Development Work for Substation and Generator Room	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	Lightning Protection System.	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	MISCELLANEOUS	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	350KVA, GENERATOR	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	Day tank for Fuel of Generator	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

23	Ancillary Equipment.	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Passive Equipment for DRDC) =							
Passive Hardware for NHQ DC							
Rack for Active Devices							
1.	Server Rack with KVM	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Rack without KVM	02	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Power Arrangement							
1.	Automatic Voltage Regulator-300KVA	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Modular Online UPS-100KVA/KW (N+2 Modules)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Floor Mounted Power Distribution System-100A with Auto transfer Switch	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	IT Power Distribution Module 3x1 Pole 3 Wire 32A	30	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	IT Power Distribution Module 3 Pole 5 Wire 32A	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	IT Power Distribution Module 3 Pole 5 Wire 63A	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Rack Automatic Transfer Switch for single corded equipment	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	Transient Voltage Surge Suppression (TVSS)	2	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Signal reference grid system	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	Data Center Earthing & Bonding system	02 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	Data Center Information Management system with Environmental	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	management system BMS						
12.	Controlled electric lighting system (Electric lighting - Intelligent Lighting System))	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Electrical Works	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	Power Cable Ladder	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	Electrical Switch Sockets	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Air Conditioning System							
1.	Precision Air Conditioner (PAC)_DX for Server Room	03 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Precision Air Conditioner (PAC)_DX for Power Room	02 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Fire Fighting System							
1.	Very early smoke detection aspirating system (VESDA)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Automated Fire Suppression system (GFSS)	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Access Control System							
1.	Access Control with visitor management System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
CCTV System							
1.	Camera	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Network Video Recorder (NVR)	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	LED TV	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Other System/ Equipment							
1.	Raised Floor	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	DC Floor Insulation	1 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Dry wall & Paint	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Water leak detection system (WDS)	01 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Lightning Protection System.	02 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Rodent System	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

7.	Fire Rated Door for Data Center	01 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	Ancillary Equipment.	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Passive Hardware for NHQ DC) =							
Passive Hardware for UDC (Command HQ & Base)							
Rack for Active Devices							
1.	Server Rack with KVM	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Rack without KVM	24	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Rack for Building (Access Switch)	300	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Rack for Floor (Access Switch)	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Power Arrangement							
1.	Stand Alone Online UPS	60	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Air Conditioning System							
2.	AC Controller	30	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Split AC (min 2.0 ton) for Room Size 200 SFT	30	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Split AC (1.5 ton)	35	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Access Control System							
1.	Access Control Reader Standalone	28 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
CCTV System (Qty: 28) for UDC and 400 for Access Switch location).							
1.	03 x 4 MP IP Bullet Camera along with 1 x 8 Channel NVR, 1x 55" LED TV & 1x 17" Monitor to be provided in each UDC.	28 Set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	02 x 2 MP IP Bullet Camera (for Building and Floor Racks)	400	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	1 x Server Based NVR software with 55" LED	28	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	TV & 1x 17" Monitor installed in the UDC server						
Other System/ Equipment							
1.	Online UPS 3KVA	300	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Online UPS 1KVA	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Ancillary Equipment.	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (UDC (Passive Equipment for Network Room))=							
Passive Hardware for UDC(Ship)							
Rack for Active Devices							
1.	Rack for UDC-SHIP (For Active Devices) 25U Floor Stand	12	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Rack for UDC-SHIP (For Active Devices) 15U Floor Stand	03	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Rack for UDC-SHIP (For Active Devices) 6U Wall Mount	42	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Rack for Ship's Jetty (For Access Switch) 12U	35	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Access Control System							
5.	Access Control Reader Standalone	15 set	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Other System/ Equipment							
6.	Online UPS 1KVA	15	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Ancillary Equipment.	As Req	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (UDC-SHIP (Passive Equipment for Network Room))=							

INFRASTRUCTURE DEVELOPMENT WORKS

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Works for DC							
1.	Works for CDC	01 set	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Works for DRDC	01 set	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Works for NHQ DC	As required	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Works for UDC-COMHQ and UDC-BASE	As required	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Works for UDC(SHIP)	As required	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Furniture's for CDC, DRDC, NHQ DC and UDC (Command HQ, Base and Ship)							
1.	Interior	As required	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Furniture and Ancillary Equipment.	As required	Local	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Misc Cost							
1.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Infrastructure Development Works) =							

COST FOR SPARES & TOOLS

Ser	Product	Qty	Brand & Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Cost for Tools Spares and Equipment's							
Tools							
1	SimpliFiber® Pro Optical Power Meter and Fiber Test Kits	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2	MultiFiber™ Pro Optical Power Meter and Fiber Test Kits	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3	OptiFiber® Pro OTDR	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4	LinkIQ Cable + Network Tester	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5	Fiber Optic Cleaning Kits	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6	Visual Fault Locator (VFL)	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7	NETWORK CABLE TESTER	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8	UTP/STP Cable Stripper	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9	Network Installation Tool Kit	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10	Repair Tools	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11	Hammer, Wrench and Drivers Tools	2 sets	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
Spares							
1	Branch Router	5	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2	Branch Firewall	5	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3	Distribution Switch	5	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4	Access Switch	20	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

5	Media Converter (10G)	20 Pair	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6	MC Rack	10	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Spares and Tools) =							

COST FOR CABLE LAYING

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Cabling Fiber & UTP (Data Center (CDC, DRDC & NHQ DC))							
1.	CAT 6A U/UTP LSZH Cable, Box of 305 mtr	253	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	Category 6A U/UTP Patch Panel, loaded, intelligent ready	304	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Category 6A U/UTP Patch Cord 10 meters	5450	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Category 6A U/UTP Patch Cord 12meters	1872	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Category 6A U/UTP Modular Information Outlets	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Work Area Faceplate	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Modular Fiber Panel 1U, Intelligent Ready	83	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
8.	Modular Fiber Panel 4U, Intelligent Ready	14	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	Pre-Terminated MPO Modules – Multimode Om4, Intelligent	608	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	2x12F MPO Trunk Cable,	46	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	OM4 10 meters						
11.	2x12F MPO Trunk Cable, OM4 12 meters	60	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	2x12F MPO Trunk Cable, OM4 15 meters	66	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	2x12F MPO Trunk Cable, OM4 18 meters	76	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	2x12F MPO Trunk Cable, OM4 20 meters	14	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	2x12F MPO Trunk Cable, OM4 22 meters	18	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	2x12F MPO Trunk Cable, OM4 25 meters	24	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	2x12F MPO Trunk Cable, OM4 30 meters	4	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
18.	LC – LC Multimode Duplex Fiber Patch Cord 8 meters	5330	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
19.	LC – LC Multimode Duplex Fiber Patch Cord 10 meters	2770	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
20.	Intelligent Upgrade Kit, Copper Panels	17	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
21.	Intelligent Upgrade Kit, Fiber Panels	33	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
22.	Intelligent Rack Controller	22	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

23.	Intelligent System Software, Per Port License	10,000	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
24.	Fiber Guide Pathway System	As Required	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
25.	Copper Wire Basket Pathway System	As Required	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
26.	Power Cable	As Required	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
27.	Overhead hanging cable tray for Network Cables	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
28.	Fiber cable runner	1	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
29.	Cable Laying Service	NA	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned

Sub-Total (Cabling Fiber & UTP at Data Center) =

Cabling Fiber & UTP (All UDCs (Command HQ, Base & Ship))

1.	CAT 6 UTP LSZH Cable, Meter	150000	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
2.	24 Port CAT6 UTP Patch Panel, loaded	400	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
3.	Category 6 UTP Modular	4800	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
4.	Category 6 UTP Patch Cord for User End 1 meter	1500	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
5.	Category 6 UTP Patch Cord for User End 2 meters	5000	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
6.	Category 6 UTP Patch Cord for User End 3 meters	400	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
7.	Category 6 UTP Patch Cord for	700	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned

RESTRICTED

	Patch Panel End						
8.	Faceplate 2 Port	700	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
9.	CAT6 Double jacketed Outdoor UV resistant Cable	9000	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
10.	CAT6 Outdoor Patch Cord 1 meter	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
11.	6 CORES – Singlemode Outside Plant Fiber Cable, Meter	16000 0	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
12.	1U Fiber Rackmount Shelf, Sliding	50	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
13.	Rolo splice kit	100	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
14.	12F LC SM Splice Cassettes	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
15.	6F SM LIU FULLY LOADED, 1U	200	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
16.	LC – LC Singlemode Duplex Fiber Patch Cord 3 meters	1000	To be mentioned	To be mentioned	To be mentioned	To be mentioned	To be mentioned
17.	Cable Laying Service	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
18.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Cabling Fiber & UTP (All UDCs) =							

COST OF DATA LINK SERVICE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Data Link (NTTN) – One Time Cost							
1.	CDC to DRDC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2.	CDC to NHQ DC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3.	NHQ DC to DRDC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
4.	CDC/NHQDC/DRDC to UDC-COMDHQ	11	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
5.	CDC/NHQDC/DRDC to UDC-BASE	17	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
6.	CDC/NHQDC/DRDC to UDC-SHIP	15	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Data Link NTTN) =							
Yearly recurring cost							
1.	CDC to DRDC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2.	CDC to NHQ DC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3.	NHQ DC to DRDC	2	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
4.	CDC/NHQDC/DRDC to UDC-COMDHQ	11	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
5.	CDC/NHQDC/DRDC to UDC-BASE	17	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
6.	CDC/NHQDC/DRDC to UDC-SHIP	15	To be mentioned	Not Applicable	Not Applicable	To be mentioned	To be mentioned
7.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Yearly Recurring Cost) =							

TRAINING PACKAGE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
1.	Foreign Training Package						
	a. Training Cost (tuition Fee)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
	b. Admin Assistance (Airfare, Boarding, Lodging and Local Transport)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2.	Local Training Package	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Training Package) =							

INSTALLATION AND ACCEPTANCE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Installation and Acceptance							
1	Installation and Acceptance	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2	Inspection (FAT and PSI)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Installation and Acceptance) =							

DATA CENTER TIER-III CERTIFICATION SERVICES

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Data Center Design Validation and Tier-3 Certification							
1	Design validation: Tier-3 from Uptime Institute USA/epi	01 Set	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2	Data Center Certification: Tier-3 from Uptime Institute USA/epi	01 set	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3.	Any other cost related to Tier certification	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Tier-III certification Services) =							

MAINTENANCE SERVICE

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Cost for Maintenance Service							

RESTRICTED

1	Maintenance support Service (5 years after the final acceptance)	05 Years	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2.	Any other cost (if any) (To be mentioned clearly)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
Sub-Total (Maintenance Service) =							

OPTIONAL ITEMS

Ser	Product	Qty	Brand& Model	Country of Origin	Country of Manufacturer	Unit Price (BDT)	Total Price (BDT)
Cost for Optional Items and Services							
1	Branch Router Type 1	02	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
2	Branch Router Type 2	03	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
3	WAN Firewall	06	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
4	Core Firewall 2	06	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
5	Branch Firewall Type 1	01	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
6	Branch Firewall Type 2	01	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
7	Branch Firewall Type 3	01	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
8	Global Server Load Balancer (GSLB) Solution & Anti DDoS with DNS Security	02	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
9	UDC POE LAN Switch	200	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
10	Distribution Switch	02	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
11	WEB Security Appliance (WSA)	02	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
12	Backup Online UPS Stand Alone- 250KVA/KW	02	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
13	Optional Items (As mentioned in various articles of the tender spec)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
14	Optional Items and Services (As mentioned in various articles of the tender spec)	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned
15	Any other cost (if any) (To be	NA	Not Applicable	Not Applicable	Not Applicable	To be mentioned	To be mentioned

RESTRICTED

mentioned clearly)					
Sub-Total (Optional Items and Services) =					