Enhancing Digital Government and Economy (EDGE) Project
Bangladesh Computer Council (BCC)
Information and Communication Technology Division
Ministry of Posts, Telecommunications and Information Technology
Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh
www.bcc.gov.bd

Memo No: 56.01.0000.046.007.086.2025- 579 Date: 16 November 2025

Project: Enhancing Digital Government and Economy (EDGE)

Contract title: Supply, Installation and Commissioning for Advanced Development of Cloud Computing Platform at National Data Center (NDC) for enhancing Digital Economy

Request for Proposals (RFP) No: EDGE-G1B

Addendum No. 1 to RFP No. EDGE-G1B

This is for the information of all concerned Proposers that the following amendments have been made to Request for Proposals (RFP) No. EDGE-G1B "Supply, Installation and Commissioning for Advanced Development of Cloud Computing Platform at National Data Center (NDC) for enhancing Digital Economy" pursuant to ITP Clause 8 of the said RFP:

Sl. No.	RFP Reference	Issued RFP	As Amended
1.	Section -II Proposal Data Sheet (PDS) ITP 23.1 Page: 46	For Proposal submission purposes only, the Purchaser's address is: Attention: Project Director, Enhancing Digital Government and Economy (EDGE) Project Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh The deadline for Proposal submission is:	For Proposal submission purposes only, the Purchaser's address is: Attention: Project Director, Enhancing Digital Government and Economy (EDGE) Project Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh The deadline for Proposal submission is: **Date: 25 November 2025**

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr><td></td><td></td><td>Date: 19 November 2025

Time: 12.00 hours Bangladesh Standard Time (BST= GMT + 6:00 hours)</td><td>Time: 12.00 hours Bangladesh Standard Time (BST= GMT + 6:00 hours)</td></tr>
<tr><td>2.</td><td>Section -II

Proposal Data Sheet (PDS)

ITP 26.1

Page: 47</td><td>The Proposal opening shall take place at:

Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh

Date: 19 November 2025

Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).</td><td>The Proposal opening shall take place at:

Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh

Date: 25 November 2025

Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).</td></tr>
<tr><td>3.</td><td>Section VII – Purchaser's Requirements

D. Technology Specifications – Supply & Install Items

3.15 DC Computing Node Server (Qty. 30 Nos)

Page No: 172, 173</td><td>3.15 DC Computing Node Server (Qty. 30 Nos)

<table><tr><th>SL</th><th>Product Names/Items</th><th>Description of requirements</th></tr><tr><td>12</td><td>Memory</td><td>- Minimum 32 DIMM slots per server
- Minimum 16x64GB DDR5 Memory with advanced ECC capability</td></tr></table></td><td>3.15 DC Computing Node Server (Qty. 20 Nos)

<table><tr><th>SL</th><th>Product Names/Items</th><th>Description of requirements</th></tr><tr><td>12</td><td>Memory</td><td>- Minimum 32 DIMM slots per server
- Minimum 32x64GB DDR5 Memory with advanced ECC capability</td></tr></table></td></tr>
<tr><td>4.</td><td>Section VII – Purchaser's Requirements</td><td>3.18 IT Rack (Qty. 6 Nos.)

<table><tr><th>SL</th><th>Product Names/Items</th><th>Description of requirements</th></tr><tr><td></td><td></td><td></td></tr></table></td><td>Dropped from the RFP</td></tr>
</table>

Sl. No.	RFP Reference	Issued RFP			As Amended
	D. Technology Specifications – Supply & Install Items 3.18 IT Rack (Qty. 6 Nos.) Page No: 177 & 178	I	Model	To be mentioned by the bidder	
		I	Country of Origin	To be mentioned by the bidder	
		I	Country of Manufacture	To be mentioned by the bidder	
		I	Standards conformed	The Cabinet should comply with the IEC 60297-2 Standard	
		I	Rack Height	The rack should have 42U	
		I	Rack Width	The width of the rack should be 800mm	
		I	Dimension	The IT cabinet dimension should not be more than 600 X 1200 X 2000mm (W X D X H)	
		I	Ventilation Rate of Front and Rear Door	The ventilation rate should not be less than 75%	
		II	Cabinet Door	The cabinet door should be 2.0mm standard perforated. Each IT rack should have perforated door with door access Finger print card swipe access control	
		II	Material	Cabinet material should be high intensity cold rolled steel plate and steel doors	
		II	Color	The color of the rack should be black	

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>[redacted]</td><td>Air channel</td><td>The air channel should be front to rear</td></tr>
<tr><td>[redacted]</td><td>Protection Grade</td><td>The protection of the rack system should be IP20</td></tr>
<tr><td>[redacted]</td><td>Warranty</td><td>Minimum 03 years comprehensive warranty</td></tr>
<tr><td>[redacted]</td><td>Installation & Commissioning</td><td>Installation, testing and commissioning with necessary accessories</td></tr>
</table>
</td><td></td></tr>
<tr><td>5.</td><td>Section VII – Purchaser's Requirements

D. Technology Specifications – Supply & Install Items

3.19 Intelligent Smart PDU (Qty. 24 Nos)

Page No: 178 & 179</td><td>3.19 Intelligent Smart PDU (Qty. 24 Nos)

<table>
<tr><th>SL</th><th>Product Names/Items</th><th>Description of requirements</th></tr>
<tr><td>1</td><td>Brand</td><td>Any Internationally reputed Brand</td></tr>
<tr><td>2</td><td>Model</td><td>To be mentioned by the bidder</td></tr>
<tr><td>3</td><td>Country of Origin</td><td>To be mentioned by the bidder</td></tr>
<tr><td>4</td><td>Country of Manufacturer</td><td>To be mentioned by the bidder</td></tr>
<tr><td>5</td><td>rPDU Type</td><td>The rPDU should be Monitoring type Rack PDU, Single Phase</td></tr>
</table>
</td><td>Number of Intelligent Smart PDU Increase:

3.18 Intelligent Smart PDU (Qty. 100 Nos.)

<table>
<tr><th>SL</th><th>Product Names/Items</th><th>Description of requirements</th></tr>
<tr><td>1</td><td>Brand</td><td>Any Internationally reputed Brand</td></tr>
<tr><td>2</td><td>Model</td><td>To be mentioned by the bidder</td></tr>
<tr><td>3</td><td>Country of Origin</td><td>To be mentioned by the bidder</td></tr>
<tr><td>4</td><td>Country of Manufacturer</td><td>To be mentioned by the bidder</td></tr>
</table>
</td></tr>
</table>

Sl. No.	RFP Reference	Issued RFP			As Amended		
		[redacted]	[redacted]	[redacted]	5	rPDU Type	The rPDU should be Monitoring type Rack PDU, Single Phase 63A full height rPDUs
		7	Capacity	The capacity should be 10.5 kVA	6	Capacity	The capacity should be 10.5 kVA
		8	Input Current	The input current should be 63A	7	Input Current	The input current should be 63A
		9	Input Rated Voltage	The input rated voltage should be 220/230/240Vac (±20%)	8	Input Rated Voltage	The input rated voltage should be 220/230/240Vac (±20%)
		10	Input Frequency	The input frequency should be 50/60Hz	9	Input Frequency	The input frequency should be 50/60Hz
		11	Indicators	The system should have 4 pcs indicators	10	Indicators	The system should have 4 pcs indicators
		12	Socket type	The PDU should be IEC socket type	11	Socket type	The PDU should be IEC socket type
		13	Output Socket	24*C13+6*C19	12	Output Socket	24*C13+6*C19
		14	Output protection	4 protection circuit breakers(16A/1P)	13	Output protection	4 protection circuit breakers(16A/1P)
		15	Monitoring capabilities	The PDU should monitor the input power, voltage, current, power factor, electric energy, and status of circuit breaker,	14	Monitoring capabilities	The PDU should monitor the input power, voltage, current, power factor, electric energy, and status of circuit breaker, Monitors main input active power and apparent power

Sl. No.	RFP Reference	Issued RFP			As Amended		
				Monitors main input active power and apparent power			- Environmental Sensor for monitoring humidity, temperature and smoke detection shall be added for each racks with necessary controller and shall be monitored from DCIM - Monitoring of the PDU must be compatible with existing DCIM or open source tools like LibreNMS at least
		16	Monitor Progress	The monitor progress should be at least 1%	15	Monitor Progress	The monitor progress should be at least 1%
		17	Operating Temperature	The operating Temperature should be 0-40°C	16	Operating Temperature	The operating Temperature should be 0-40°C
		18	Storage Temperature	The storage Temperature should be -20-70°C	17	Storage Temperature	The storage Temperature should be -20-70°C
		19	Relative Humidity	The relative humidity should be 5%-95%	18	Relative Humidity	The relative humidity should be 5%-95%
		20	Installation Type	the system should be Full-height vertical installation	19	Installation Type	the system should be Full-height vertical installation
		21	Certification	The system should be CE, UKCA, EMC, LVD, certified.	20	Certification	The system should be CE, UKCA, EMC, LVD, certified.
		22	Compatibility	The Item must be compatible and integrate-able with any standard IT rack including the proposed rack			
		23	Warranty	Minimum 03 years comprehensive warranty from the date of commissioning with OEM support			

Sl. No.	RFP Reference	Issued RFP	As Amended
		24 | Installation& Commissioning | Installation, testing and commissioning with necessary accessories	21 | Compatibility | The Item must be compatible and integrate-able with any standard IT rack including the proposed rack. The PDU must be compatible with any rack having width of 600mm/800mm and depth of 800mm/1000mm/1200mm. 22 | Warranty | Minimum 03 years comprehensive warranty from the date of commissioning with OEM support 23 | Installation& Commissioning | Installation, testing and commissioning with necessary accessories
6.	Section VII – Purchaser's Requirements D. Technology Specifications – Supply & Install Items 3.20 Service Level Agreement (SLA) Page No: 179, 180	3.20 Service Level Agreement (SLA)	3.24 Service Level Agreement (SLA)

Sl. No.	RFP Reference	Issued RFP	As Amended
7.	Section VII – Purchaser's Requirements D. Technology Specifications – Supply & Install Items 3.1.25.1 Additional Provisions Page No: 180	3.1.25.1 Additional Provisions	3.24.1 Additional Provisions
8.	Section VII – Purchaser's Requirements D. Technology Specifications – Supply & Install Items	-	3.24.2 Special Technical Instructions - Ensure monitoring of all the infrastructure items within scope of this package under existing monitoring system, - Dashboard & Reporting shall be available for all the solution/item within the scope of this package, - All necessary license shall be added to enable monitoring and visibility of the offered solution and products
9.	**ITP 32.2** **Page No: 47**	The weighting to be given for Rated Criteria (including technical and non-price factors) is: *40%*. The technical factors (including sub-factors if any), which for purposes of this document carry the same meaning as	The weighting to be given for Rated Criteria (including technical and non-price factors) is: *40%*. The technical factors (including sub-factors if any), which for purposes of this document carry the same meaning as Rated Criteria, and the corresponding weight out of 100% are:

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr>
<td></td>
<td></td>
<td>Rated Criteria, and the corresponding weight out of 100% are:
<table>
<tr><th>Sl.No.</th><th>Technical Factor</th><th>Weight in percentage (Weight in %)</th><th>Reference</th></tr>
<tr><td>1</td><td>Preliminary Project Plan addressing the required topics.</td><td>25%</td><td>Section IV – Proposal Forms, Format of the Technical Proposal</td></tr>
<tr><td>2</td><td>Cyber security management strategies and implementation plans</td><td>25%</td><td>Section IV – Proposal Forms, Format of the Technical Proposal</td></tr>
<tr><td>3</td><td>Preferred: Scalability Requirements Future-Ready Features Energy Efficiency</td><td>25%</td><td>Part -2, Purchaser's Technical Requirements Section VII. Preferred: mentioned in the section 3.1 Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set), A. Addition of New Cloud Services in eGov Cloud Platform of</td></tr>
</table>
</td>
<td>
<table>
<tr><th>Sl.No.</th><th>Technical Factor</th><th>Weight in percentage (Weight in %)</th><th>Reference</th></tr>
<tr><td>1</td><td>Preliminary Project Plan addressing the required topics.</td><td>25%</td><td>Section IV – Proposal Forms, Format of the Technical Proposal</td></tr>
<tr><td>2</td><td>Cyber security management strategies and implementation plans</td><td>25%</td><td>Section IV – Proposal Forms, Format of the Technical Proposal</td></tr>
<tr><td>3</td><td>Preferred: Scalability Requirements Future-Ready Features Energy Efficiency</td><td>25%</td><td>Part -2, Purchaser's Technical Requirements Section VII. Preferred: mentioned in the section 3.1 Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set), A. Addition of New Cloud Services in eGov Cloud Platform of NDC, serial: 15,16 and 17.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>NDC, serial: 13,14 and 15.</td></tr>
<tr><td>4</td><td>Preferred: Gartner Magic Quadrant-Based Product Evaluation</td><td>25%</td><td>Part-2, Purchaser's Technical Requirements Section VII: Preferred: mentioned in Gartner Magic Quadrant-Based Product Evaluation' under the section 3.2 to 3.7.</td></tr>
<tr><td></td><td>Total</td><td>100%</td><td></td></tr>
</table>
The technical proposal scoring methodology is specified in Section III- Evaluation and Qualification Criteria.
</td><td>
<table>
<tr><td>4</td><td>Preferred: Gartner Magic Quadrant-Based Product Evaluation</td><td>25%</td><td>Part-2, Purchaser's Technical Requirements Section VII: Preferred: mentioned in Gartner Magic Quadrant-Based Product Evaluation' under the section 3.2 to 3.7.</td></tr>
<tr><td></td><td>Total</td><td>100%</td><td></td></tr>
</table>
The technical proposal scoring methodology is specified in Section III- Evaluation and Qualification Criteria.
</td></tr>
<tr><td>10.</td><td>SECTION III - EVALUATION AND QUALIFICATION CRITERIA (WITHOUT PREQUALIFICATION), 2. Technical Evaluation 2.2 Technical Evaluation (ITP 32.2)

Page No: 56</td><td>
<table>
<tr><th>Sl.No.</th><th>Technical Factor</th><th>Weight in percentage (Weight in %)</th></tr>
<tr><td>1</td><td>Preliminary Project Plan addressing the required topics.</td><td>25%</td></tr>
<tr><td>2</td><td>Cyber security management strategies and implementation plans</td><td>25%</td></tr>
<tr><td>3</td><td>Preferred:
Scalability Requirements
Future-Ready Features
Energy Efficiency</td><td>25%</td></tr>
</table>
</td><td>
<table>
<tr><th>Sl.No.</th><th>Technical Factor</th><th>Weight in percentage (Weight in %)</th></tr>
<tr><td>1</td><td>Preliminary Project Plan addressing the required topics.</td><td>25%</td></tr>
<tr><td>2</td><td>Cyber security management strategies and implementation plans</td><td>25%</td></tr>
<tr><td>3</td><td>Preferred:
Scalability Requirements
Future-Ready Features
Energy Efficiency</td><td>25%</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>Under the section 3.1 (A), serial: 13,14 and 15.</td><td></td></tr>
<tr><td>4</td><td>Preferred:
Gartner Magic Quadrant-Based
Product Evaluation
Under the section 3.2 to 3.7.</td><td>25%</td></tr>
<tr><td></td><td>Total</td><td>100%</td></tr>
</table>
</td><td>
<table>
<tr><td></td><td>Under the section 3.1 (A), serial: 15,16 and 17.</td><td></td></tr>
<tr><td>4</td><td>Preferred:
Gartner Magic Quadrant-Based
Product Evaluation
Under the section 3.2 to 3.7.</td><td>25%</td></tr>
<tr><td></td><td>Total</td><td>100%</td></tr>
</table>
</td></tr>
<tr><td>11.</td><td>Section VII – Purchaser's Requirements
C. Service Specifications – Supply & Install Items
2.3 Knowledge Transfer
Page No: 135</td><td>2.3 Knowledge Transfer
2.3.1 The Supplier MUST provide following knowledge transfer services:
(1) Pre-deployment workshop on the HLD and LLD in BCC
(2) Pre-deployment knowledge transfer program on the entire platform for 10 persons in BCC lab facilities
(3) Hands-on post-deployment knowledge transfer program for 10 persons in BCC lab facilities</td><td>2.3 Knowledge Transfer
2.3.1 The Supplier MUST provide following knowledge transfer services:
<table>
<tr><th>SL</th><th>Types of Session & Location</th><th>Number of Participants</th><th>Duration</th></tr>
<tr><td>1</td><td>Pre-deployment workshop on the HLD and LLD in BCC or EDGE Project Office</td><td>50</td><td>1 Day (1 Session)</td></tr>
<tr><td>2</td><td>Pre-deployment knowledge transfer program on the</td><td>10</td><td>3 Days (9 Session)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Sl. No.</th><th>RFP Reference</th><th>Issued RFP</th><th>As Amended</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>entire platform in BCC or EDGE Project Office</td><td></td><td></td></tr>
<tr><td>3</td><td>Hands-on post-deployment knowledge transfer program in BCC or EDGE Project Office</td><td>10</td><td>5 Days (15 Session)</td></tr>
</table>
</td></tr>
</table>

SL. No. 10

Section VII – Purchaser's Requirements

D. Technology Specifications – Supply & Install Items

3.1 (A) Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)

Page No: 136-145

As in issued RFP

3.1 Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)

A. Addition of New Cloud Services in eGov Cloud Platform of NDC

SL	Product Names/Items	Description of requirements
1	Distributed Database Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 256 cloud software licenses for Cloud Database Service - The distributed database should use the shared-nothing and massively parallel processing (MPP) architectures to support horizontal scaling - The distributed database should provide strong consistency of distributed transactions - The distributed database should support stored procedures, functions, and views - The distributed database should support large object types, including CLOB, TEXT, and BLOB. The maximum size of BLOB data types support shall be 1 GB - The distributed database should support JDBC client-based and ELB-based load balancing - The distributed database should support scale-out capabilities, allowing expansion up to 256 shards - The distributed database should support distributed CBO optimizer. - The distributed database should support online scale-out without downtime - The distributed database should support online node replacement. During node replacement, online DDL and DML operations can be executed to prevent service interruption - The distributed database should support comprehensive security protection capabilities, including transparent data encryption (KMS-based), SSL encryption and dynamic data masking - The distributed database should support user permission and fine-grained permission management - The distributed database should support database-level and table-level backup and restoration - The distributed database should allow users to move deleted instances to the recycle bin. Users can rebuild DB instances in the recycle bin within the retention period to restore data
2	Relational Database Service (with PostgreSQL)	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 384 cloud software licenses for RDS for PgSQL.

SL	Product Names/Items	Description of requirements
		- The proposed PostgreSQL database should support mainstream PostgreSQL versions 13, 14, 15, 16 and 17 - The proposed PostgreSQL database should support single-node instance and primary/standby instance - The proposed PostgreSQL database should support for backup and custom backup policy - The proposed PostgreSQL database should support database-level and table-level PITR - The proposed PostgreSQL database should support for SQL Audit Log
3	Bare Metal Computing Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 10 cloud software licenses for Cloud Bare Metal Service - The proposed solution should allow users to request Windows or Linux bare metal servers on the management platform to run their workloads. Users can configure the flavor, image, network, security group, EIP, and login information, as well as add multiple data disks and set some of the data disks as shared disks for a bare metal server when requesting the bare metal server - The proposed solution should support user data injection during bare metal server provisioning to complete OS initialization configurations, such as host name and password injection - After a bare metal server request is submitted, the proposed solution should support the configuration of a security group and IP address, and binds an EIP to the bare metal server automatically - The proposed solution should support bare metal server lifecycle management and related service operations, such as starting, stopping, restarting, deleting, and monitoring bare metal servers. When deleting a bare metal server, users can determine whether to delete data disks of the bare metal server - The proposed bare metal server should support centralized SAN storage such as NoF SAN, IP SAN, or FC SAN - The proposed bare metal server supports the attachment of block storage disks as data disks. Users can attach these disks directly through the bare metal server management console during provisioning, without needing to access the storage management console - The proposed bare metal server should support shared storage, allowing a single disk to be attached to two bare metal servers simultaneously - The proposed bare metal server support provisioning servers with local disks - In the proposed solution, bare metal servers and cloud servers can share the same VPC and subnet - The proposed bare metal server solution should support RoCE networks
4	Cloud Endpoint Security Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 500 cloud software licenses for Cloud Endpoint Security Service and 200 cloud software license for container security.

SL	Product Names/Items	Description of requirements
		- The agent in the proposed Cloud Endpoint Security Service, should be light-weight. The agent when running, should not affect the system performance - The proposed Cloud Endpoint Security Service should be able to count and display information such as host account permissions, user groups, user directories, startup shells, process paths, startup parameters, file permissions, file hashes, open ports, self-startup item paths and running users - The proposed Cloud Endpoint Security Service should be able to count and display web application information, such as the web application versions, software directories, configuration files and associated process paths. Moreover, it should showcase website information, such as external domain names, port numbers, URLs and directories - The proposed Host-Based (Endpoint) Security Service should be capable of identifying and displaying middleware details, including versions, installation paths, and related process paths, as well as database information such as versions, installation paths, configuration files, and associated processes - The proposed Cloud Endpoint Security Service should detect vulnerabilities of Windows and Linux OSs, applications, third-party components related to applications, and Web-CMS. The EDR should display the vulnerability name, risk level, description, and details, and provides repair suggestions and batch repair capabilities - The proposed Cloud Endpoint Security Service should provide description of processes affected by the vulnerability, including Common Vulnerabilities and Exposures details - The proposed Cloud Endpoint Security Service should support password complexity policy check, scans system and application accounts based on the weak password dictionary, reports weak passwords and how long they are used, and prompts users to change the passwords. The weak password dictionary can be customized - The proposed Cloud Endpoint Security Service should detect risky configurations based on graded protection requirements, identifies insecure configurations of common operating systems and middleware; such as Windows, Linux, Apache, Tomcat, Docker, MongoDB, MySQL, Redis, Nginx, SSH, and provides modification suggestions - The proposed Cloud Endpoint Security Service should detect brute-force attacks. The identified attack source IP addresses can be blocked for 12 hours to prevent them from logging in to the system again, preventing hosts intrusion - The proposed Cloud Endpoint Security Service should detect threats such as web shells, reverse shells, abnormal shells, high-risk command execution, suspicious Crontab tasks, suspicious system accounts, and abnormal privilege escalation operations - The proposed Cloud Endpoint Security Service should allow users to set common login locations and IP addresses, detect remote logins to servers and logins from abnormal IP addresses, and generate alarms

SL	Product Names/Items	Description of requirements
		- The proposed Cloud Endpoint Security Service should supports malicious program detection (cloud-based virus scan and removal): The latest malicious program database and multiple virus scan and removal engines are used. The program database (used to scan and remove known malicious programs), image fingerprint algorithms (which can scan for and remove variants based on AI), and cloud-based virus scan and removal are used to detect and remove viruses, Trojans, web shells, worms, and mining software in running processes, and to provide one-click isolation and removal capabilities - The proposed Cloud Endpoint Security Service should have Ransomware detection, isolation, scan, and blocking, as well as backup and restoration after a ransomware attack are supported - The proposed Cloud Endpoint Security Service should have virus detection engine, which can scan for viruses on the server. It scans for weak system modules, such as active processes, hidden processes, kernel modules, installed programs, dynamic library hijacking, scheduled tasks, startup items, sensitive directories, office files, images, videos, execution scripts, and compressed packages. Moreover, users can perform quick scan, full scan, and custom scan tasks on cloud servers to detect, isolate, and kill viruses based on policies. - The proposed Host-Based (Endpoint) Security Service should include application protection powered by RASP technology, offering security defenses for active applications. It should detect threats such as SQL injection, OS command injection, XSS attacks, web shells, Log4j injection, and other similar exploits across various application scenarios, ensuring robust protection for running applications - The proposed Cloud Endpoint Security Service should allow users to mitigate and handle alarms based on the alarm whitelist and policies. Moreover, it should be able to collect statistics on alarms based on the attack status, such as system vulnerabilities, abnormal behaviors, attack attempts, blocked attacks, successful attacks, and server intrusions - The proposed Cloud Endpoint Security Service should allow users to create, copy, generate, display, and download security reports (including daily, weekly, monthly, and custom security reports). The security report must contain at least the risk trend, risk distribution, vulnerability status, dangerous open ports, weak passwords, risky accounts, malicious programs, and key file changes. The report can be customized and tailored - The proposed Cloud Endpoint Security Service should allow users to modify and view detection policies, customize and deliver detection policies, and flexibly configure detection policies for each group or each server, facilitating refined security operation - The proposed Cloud Endpoint Security Service should supports Windows, CentOS, Ubuntu, Debian and SUSE.
5	Cloud Bastion Host Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 200 Assets cloud software license for Cloud Bastion Host Service

SL	Product Names/Items	Description of requirements
		- The proposed Cloud Bastion Host Service should enable customers to configure multi-factor authentication, such as mobile phone one-time passwords (OTPs), mobile phone SMS messages, USB keys, and dynamic OTP tokens, to authenticate user identities. O&M accounts can be authenticated through AD, RADIUS, LDAP, and Azure AD platforms - The proposed Cloud Bastion Host Service should enable customers to configure resource access control rules based on users, user groups, managed accounts, and account groups to limit what resources can be assessed. Moreover, customers should also be able to configure two-person authorization policies and command control policies to limit what operations are allowed on a certain resource - The proposed Cloud Bastion Host Service should enable customers to set resource access permissions in many ways, including the access validity period, login time range, IP address restriction, upload and download control, file transfer, clipboard, and watermarking - The proposed Cloud Bastion Host Service should enable customers to set command or database control policies to manage and control key operations. When a sensitive or high-risk operation is performed, the system response must include at least dynamic authorization, forcible blocking, alarm reporting, and secondary review - The proposed Cloud Bastion Host Service, should enable resource management for VMs through automatic resource discovery, one-click synchronization of cloud resources, and batch import of resources from files - The proposed Cloud Bastion Host Service, should enable resource management for Kubernetes containers - The proposed Cloud Bastion Host Service should allow passwords of resource accounts to be automatically changed. Customers can configure password change policies and specify when and how the policies work. A password change policy can be triggered manually, as scheduled, or periodically. Logs for password changes can be queried and downloaded. Resource accounts include the ones for host resources that have SSH, RDP, SMB, or Telnet enabled and accounts for database resources of many types such as MySQL, SQL Server, Oracle, PostgreSQL, GaussDB - The proposed Cloud Bastion Host Service should enable customers to configure account synchronization policies to let the system detect zombie accounts or unmanaged accounts in a timely manner - The proposed Cloud Bastion Host Service should allow Linux commands and Windows operations to be recorded by screen recordings. In this case, the idle duration in recordings can be filtered out and video recordings can be downloaded in just a few clicks - The proposed Cloud Bastion Host Service should support Centralized display of O&M statistics, including O&M action distribution over time, resource access times, session duration,

SL	Product Names/Items	Description of requirements
		command interception, number of commands, and number of transferred files. O&M reports can be exported in one click - The proposed Cloud Bastion Host Service should allow Two-person authorization, also called treasury mode. After two-person authorization is configured, O&M personnel can access core resources only after being authorized and authenticated by the administrator onsite - The proposed Cloud Bastion Host Service should enable System login-logs, resource login-logs, command execution-logs, file operation-logs, and two-person authorization logs to be remotely backed up to Syslog servers. System configuration-logs and session recording playback-logs can be remotely backed up to FTP or SFTP servers. - The proposed Cloud Bastion Host Service should enable customers to upload and download files via a browser, as well as share files from a Jump Server instance with the cloud servers it manages - The proposed Cloud Bastion Host Service should allow O&M engineers to log in to multiple authorized resources in one click. Moreover, multiple resources should be able to operate and maintain on the same browser tab page at the same time. Along with that, O&M engineers should be able to execute an O&M command for a group of resources concurrently - The proposed Cloud Bastion Host Service should allow O&M engineers to invite other engineers to join the same session for collaborative O&M and skill sharing - The proposed Cloud Bastion Host Service should enable scripts to be managed and edited in the Jump Server. Moreover, customers should be able to configure automated O&M tasks to let Jump Server automatically execute one or more preset O&M tasks, such as command execution, script execution, and file transfer tasks - The proposed Cloud Bastion Host Service should enable customers to apply for access and command authorization tickets. Moreover, customers should be able to obtain the resource control permissions by manually or automatically triggering a system ticket and submitting the ticket for approval - The proposed Cloud Bastion Host Service should enable customers to create custom approval processes. Along with that, multi-level approval, countersign approval, and multi-person approval should also be supported
6	Cloud Network Detection & Response (NDR) Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 1 Set of 10 GBP/s cloud software license of Cloud NDR Service - The proposed Cloud NDR Service should support heavy traffic detection and identification of typical application protocols, such as HTTP, TCP, UDP, DNS, SMTP, DHCP, FTP, MySQL, IMAP, SSH, SMB, RDP, Telnet, TLS, MSSQL, etc. - The proposed Cloud NDR Service should support identification and defense against typical attacks, such as brute force cracking, scanning, web attacks, web shells, reverse shells, malicious

SL	Product Names/Items	Description of requirements
		programs, abnormal connections, abnormal protocols, and data leakage - The proposed Cloud NDR Service should allow users to set the working mode, including the observation mode and interception mode - The proposed Cloud NDR Service should allow users to set blacklists and whitelists by IP address or IP address segment, and supports batch importing and exporting of blacklists and whitelists - The proposed Cloud NDR Service should support user access behavior audit, including middleware application access audit, high-risk protocol request connection audit, and hacker tool connection audit. The fields of behavior audit should include the time, risk level, alarm credibility, project ID, tenant name, rule ID, matched rule name, attack source IP address, attack source port, attacked IP address, attacked port, transmission protocol, application protocol, and direction - The proposed Cloud NDR Service should support rule signature engine, behavior analysis engine, machine learning engine, and authoritative third-party rule signature libraries, which can be uploaded offline at any time to improve the security detection rate and accuracy. - The proposed Cloud NDR Service should determine the source of attacks using the geographical location information library; loads offline update packages as required to access the most up-to-date intelligence, enabling swift analysis of attacks - The proposed Cloud NDR Service should provide visualizations of the global distribution of attackers, details of attack techniques, top attack sources, and the complete attack paths of individual attackers, including timelines, MITRE ATT&CK matrix representations, attack relationship Sankey diagrams, and in-depth attacker profiles. It should enable automatic or manual association of IP addresses to uncover common attack strategies and related attackers, and allow the downloading of PCAP files associated with attacks for comprehensive analysis - The proposed Cloud NDR Service should support north-south traffic detection at the Internet egress, cross-VPC traffic detection, and traffic detection between VMs on the same network segment in a VPC - The proposed Cloud NDR Service should provide detailed visualized security charts which displays key detection and response information in the entire attack defense process, including alarm response trend, total number of alarms, total number of detected alarms, number of attacked IP addresses, number of attacking IP addresses, alarm risk type distribution, alarm reliability distribution, alarm risk level distribution, alarm trend, top 5 attacker distribution, top 5 attack types, top 5 attacked IP addresses, and top 5 attackers (based on attacked IP addresses), number of attack responses, number of blocked attacks, number of blocked IP addresses, number of new whitelisted IP addresses, IP address status distribution, attack response distribution, blocking type distribution, attack response

SL	Product Names/Items	Description of requirements
		trend, distribution of top 5 blocked IP addresses, and top 5 blocked IP addresses. - The proposed Cloud NDR Service should allow users to view and search logs and attack alarms; provides IP address blocking and attack interception; and integrates developed graphical rule response system to respond to new threats within seconds. - The proposed Cloud NDR Service should support the search and analysis of traffic logs and attack logs and generates reports based on threat events, traffic statistics, and protocol statistics. Moreover, attack logs can display information such as the username, project ID, matched rule, quintuple, and attack payload of the attacked host.
7	Database Audit Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 4 set of cloud software licenses (each set contains 5 Databases license) for Database Audit Security Service - The proposed database audit service should audit all operations (such as, insert, delete, update, and user-defined) on mainstream database systems in real time. The restoration operation information includes the session ID, database instance, database type, database user, client MAC address, database MAC address, client IP address, database IP address, client port, database port, client name, operation type, operation object type, response result, number of affected rows, start time, end time, SQL request statement, and request result fields. Agents can be installed for audit in CCE clusters. - The proposed database audit service should display the database audit information, including the device and host information of sessions and operation information - The proposed database audit service should display auditing information in multiple dimensions, such as session, statement, and behavior. Audit logs can be searched based on fields such as the client IP address, client name, database IP address, database user, operation type, rule name, and SQL statement keyword - The proposed database audit service should aggregate audit information of all managed databases across audit instances, including statement distribution, risk distribution, risk rule analysis, and session distribution, and displayed on the user interface - The proposed database audit service should provide report templates, including database security general report, database security compliance report, SOX report, database server analysis report, client IP address analysis report, DML command report, DDL command report, and DCL command report - The proposed database audit service should allow audit reports to be exported in PDF format -
8	Cloud Next Generation Firewall	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 5 cloud software licenses for Cloud Firewall Security Service. - The proposed cloud firewall should come with Access Control List (ACL) capability. Access control policies can be configured

SL	Product Names/Items	Description of requirements
		based on 5-tuple, address group, service group, and blacklist and whitelist. A protection rule contains at least the direction, source type, source address, destination type, destination address, service type, protocol type, source port, destination port, and IP location. For the blacklist and whitelist, you can set the address direction, IP address, port number, and protocol type. You can enter one or more IP addresses. A maximum of 100 IP addresses can be parsed at a time. Service groups can be configured and added by protocol, source port, and destination port. Pre-defined address groups and pre-defined service groups are supported. Traffic can be controlled based on 10+ application layer protocols - The proposed cloud firewall should support access control based on domain names or wildcard domain names. Users can add a domain name group of the website filtering type or DNS resolution type - The proposed cloud firewall should support access control over Internet border traffic, traffic between VPCs, and traffic between VPCs and Direct Connect gateways, as well as inbound and outbound traffic - The proposed cloud firewall should support intrusion prevention system (IPS), displays IPS signatures (attack type, severity, and impact scope), and supports the detection mode and block mode. Each IPS signature can be enabled and disabled. The blocking mode can be strict, moderate, or loose. Supports the antivirus function - The proposed cloud firewall should support virus defense, identifying and handling virus-infected files in traffic via HTTP, SMTP, POP3, FTP, IMAP4, and SMB protocols - The proposed cloud firewall should support proactive external connection analysis, proactively detects abnormal behaviors of cloud servers, collects external connection traffic statistics, and displays attack trends - The proposed cloud firewall should support the analysis of Internet-to-service access traffic, including Internet inbound and outbound traffic, attack trend, and top access IP addresses - The proposed cloud firewall should record intrusion event logs, traffic logs, and access control logs. Attack event logs include the occurrence time, attack type, risk level, rule ID, source IP address, source port, destination IP address, destination port, protocol, and application. Access control logs contain at least the receiving time, access source, source port, destination IP address, destination port, protocol, response action, and rule. Traffic logs contain at least the start/end time, access source, source port, destination IP address, destination port, protocol, number of stream bytes, and number of stream packets.
9	Integration with Existing Systems	Provide seamless integration including all necessary license as mentioned with existing eGov Cloud Platform in BCC NDC, ensuring compatibility with current infrastructure, workflows, and resource pools.
10	Reference Document	Performance and compliance reference documents related to the proposed solution should be included in the proposer's submission.

SL	Product Names/Items	Description of requirements
11	Warranty	The manufacturer's warranty must be specified, and a minimum warranty period of three (03) years should be offered for this solution starting from the date of commissioning.
12	Installation & Commissioning	Installation, testing, and commissioning must be carried out by the OEM, and the proposer is required to supply all necessary accessories needed for the installation and commissioning process.
13	Preferred: Scalability Requirements	• The solution must support modular and scalable infrastructure to accommodate future growth in data demands. • The architecture should enable seamless scaling of the following components: o Storage: Expansion of storage capacity in increments, up to at least 100% of the initial capacity without downtime or disruption to existing services. o Compute: Horizontal and vertical scaling of compute resources to meet future workload requirements. o Network: Support for increased bandwidth, additional virtual networks, and enhanced network throughput as required. • The platform must ensure compatibility with new hardware or software components for scaling purposes
14	Preferred: Future-Ready Features	• Software-Defined Infrastructure: The solution must leverage software-defined technologies (e.g., software-defined storage, networking) to facilitate dynamic resource allocation and easy integration of additional components. • Monitoring and Automation: Provide tools to monitor resource usage and automate scaling based on predefined thresholds.
15	Preferred: Energy Efficiency	• The proposed solution must align with energy efficient practices: o Equipment must comply with Energy Star® standards or equivalent certifications for energy efficiency. o Include options for dynamic power management to optimize power consumption based on workload.

As Amended

3.1 Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)

B. Addition of New Cloud Services in eGov Cloud Platform of NDC

SL	Product Names/Items	Description of requirements
1	Distributed Database Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 256 cloud software licenses for Cloud Database Service - The distributed database should use the shared-nothing and massively parallel processing (MPP) architectures to support horizontal scaling - The distributed database should provide strong consistency of distributed transactions - The distributed database should support stored procedures, functions, and views - The distributed database should support large object types, including CLOB, TEXT, and BLOB. The maximum size of BLOB data types support shall be 1 GB - The distributed database should support JDBC client-based and ELB-based load balancing - The distributed database should support scale-out capabilities, allowing expansion up to 256 shards - The distributed database should support distributed CBO optimizer. - The distributed database should support online scale-out without downtime - The distributed database should support online node replacement. During node replacement, online DDL and DML operations can be executed to prevent service interruption - The distributed database should support comprehensive security protection capabilities, including transparent data encryption (KMS-based), SSL encryption and dynamic data masking - The distributed database should support user permission and fine-grained permission management - The distributed database should support database-level and table-level backup and restoration - The distributed database should allow users to move deleted instances to the recycle bin. Users can rebuild DB instances in the recycle bin within the retention period to restore data
2	Relational Database Service (with PostgreSQL)	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 384 cloud software licenses for RDS for PgSQL. - The proposed PostgreSQL database should support mainstream PostgreSQL versions 13, 14, 15, 16 and 17 - The proposed PostgreSQL database should support single-node instance and primary/standby instance - The proposed PostgreSQL database should support for backup and custom backup policy - The proposed PostgreSQL database should support database-level and table-level PITR

SL	Product Names/Items	Description of requirements
		- The proposed PostgreSQL database should support for SQL Audit Log
3	Bare Metal Computing Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 10 cloud software licenses for Cloud Bare Metal Service - The proposed solution should allow users to request Windows or Linux bare metal servers on the management platform to run their workloads. Users can configure the flavor, image, network, security group, EIP, and login information, as well as add multiple data disks and set some of the data disks as shared disks for a bare metal server when requesting the bare metal server - The proposed solution should support user data injection during bare metal server provisioning to complete OS initialization configurations, such as host name and password injection - After a bare metal server request is submitted, the proposed solution should support the configuration of a security group and IP address, and binds an EIP to the bare metal server automatically - The proposed solution should support bare metal server lifecycle management and related service operations, such as starting, stopping, restarting, deleting, and monitoring bare metal servers. When deleting a bare metal server, users can determine whether to delete data disks of the bare metal server - The proposed bare metal server should support centralized SAN storage such as NoF SAN, IP SAN, or FC SAN - The proposed bare metal server supports the attachment of block storage disks as data disks. Users can attach these disks directly through the bare metal server management console during provisioning, without needing to access the storage management console - The proposed bare metal server should support shared storage, allowing a single disk to be attached to two bare metal servers simultaneously - The proposed bare metal server support provisioning servers with local disks - In the proposed solution, bare metal servers and cloud servers can share the same VPC and subnet - The proposed bare metal server solution should support RoCE networks
4	Cloud Endpoint Security Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 500 cloud software licenses for Cloud Endpoint Security Service and 200 cloud software license for container security. - The agent in the proposed Cloud Endpoint Security Service, should be light-weight. The agent when running, should not affect the system performance - The proposed Cloud Endpoint Security Service should be able to count and display information such as host account permissions, user groups, user directories, startup shells, process paths, startup

SL	Product Names/Items	Description of requirements
		parameters, file permissions, file hashes, open ports, self-startup item paths and running users - The proposed Cloud Endpoint Security Service should be able to count and display web application information, such as the web application versions, software directories, configuration files and associated process paths. Moreover, it should showcase website information, such as external domain names, port numbers, URLs and directories - The proposed Host-Based (Endpoint) Security Service should be capable of identifying and displaying middleware details, including versions, installation paths, and related process paths, as well as database information such as versions, installation paths, configuration files, and associated processes - The proposed Cloud Endpoint Security Service should detect vulnerabilities of Windows and Linux OSs, applications, third-party components related to applications, and Web-CMS. The EDR should display the vulnerability name, risk level, description, and details, and provides repair suggestions and batch repair capabilities - The proposed Cloud Endpoint Security Service should provide description of processes affected by the vulnerability, including Common Vulnerabilities and Exposures details - The proposed Cloud Endpoint Security Service should support password complexity policy check, scans system and application accounts based on the weak password dictionary, reports weak passwords and how long they are used, and prompts users to change the passwords. The weak password dictionary can be customized - The proposed Cloud Endpoint Security Service should detect risky configurations based on graded protection requirements, identifies insecure configurations of common operating systems and middleware; such as Windows, Linux, Apache, Tomcat, Docker, MongoDB, MySQL, Redis, Nginx, SSH, and provides modification suggestions - The proposed Cloud Endpoint Security Service should detect brute-force attacks. The identified attack source IP addresses can be blocked for 12 hours to prevent them from logging in to the system again, preventing hosts intrusion - The proposed Cloud Endpoint Security Service should detect threats such as web shells, reverse shells, abnormal shells, high-risk command execution, suspicious Crontab tasks, suspicious system accounts, and abnormal privilege escalation operations - The proposed Cloud Endpoint Security Service should allow users to set common login locations and IP addresses, detect remote logins to servers and logins from abnormal IP addresses, and generate alarms - The proposed Cloud Endpoint Security Service should supports malicious program detection (cloud-based virus scan and removal): The latest malicious program database and multiple virus scan and removal engines are used. The program database (used to scan and remove known malicious programs), image fingerprint algorithms (which can scan for and remove variants based on AI), and cloud-based virus scan and removal are used to

SL	Product Names/Items	Description of requirements
		detect and remove viruses, Trojans, web shells, worms, and mining software in running processes, and to provide one-click isolation and removal capabilities - The proposed Cloud Endpoint Security Service should have Ransomware detection, isolation, scan, and blocking, as well as backup and restoration after a ransomware attack are supported - The proposed Cloud Endpoint Security Service should have virus detection engine, which can scan for viruses on the server. It scans for weak system modules, such as active processes, hidden processes, kernel modules, installed programs, dynamic library hijacking, scheduled tasks, startup items, sensitive directories, office files, images, videos, execution scripts, and compressed packages. Moreover, users can perform quick scan, full scan, and custom scan tasks on cloud servers to detect, isolate, and kill viruses based on policies. - The proposed Host-Based (Endpoint) Security Service should include application protection powered by RASP technology, offering security defenses for active applications. It should detect threats such as SQL injection, OS command injection, XSS attacks, web shells, Log4j injection, and other similar exploits across various application scenarios, ensuring robust protection for running applications - The proposed Cloud Endpoint Security Service should allow users to mitigate and handle alarms based on the alarm whitelist and policies. Moreover, it should be able to collect statistics on alarms based on the attack status, such as system vulnerabilities, abnormal behaviors, attack attempts, blocked attacks, successful attacks, and server intrusions - The proposed Cloud Endpoint Security Service should allow users to create, copy, generate, display, and download security reports (including daily, weekly, monthly, and custom security reports). The security report must contain at least the risk trend, risk distribution, vulnerability status, dangerous open ports, weak passwords, risky accounts, malicious programs, and key file changes. The report can be customized and tailored - The proposed Cloud Endpoint Security Service should allow users to modify and view detection policies, customize and deliver detection policies, and flexibly configure detection policies for each group or each server, facilitating refined security operation - The proposed Cloud Endpoint Security Service should supports Windows, CentOS, Ubuntu, Debian and SUSE.
5	Cloud Bastion Host Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 200 Assets cloud software license for Cloud Bastion Host Service - The proposed Cloud Bastion Host Service should enable customers to configure multi-factor authentication, such as mobile phone one-time passwords (OTPs), mobile phone SMS messages, USB keys, and dynamic OTP tokens, to authenticate user identities. O&M accounts can be authenticated through AD, RADIUS, LDAP, and Azure AD platforms

SL	Product Names/Items	Description of requirements
		- The proposed Cloud Bastion Host Service should enable customers to configure resource access control rules based on users, user groups, managed accounts, and account groups to limit what resources can be assessed. Moreover, customers should also be able to configure two-person authorization policies and command control policies to limit what operations are allowed on a certain resource - The proposed Cloud Bastion Host Service should enable customers to set resource access permissions in many ways, including the access validity period, login time range, IP address restriction, upload and download control, file transfer, clipboard, and watermarking - The proposed Cloud Bastion Host Service should enable customers to set command or database control policies to manage and control key operations. When a sensitive or high-risk operation is performed, the system response must include at least dynamic authorization, forcible blocking, alarm reporting, and secondary review - The proposed Cloud Bastion Host Service, should enable resource management for VMs through automatic resource discovery, one-click synchronization of cloud resources, and batch import of resources from files - The proposed Cloud Bastion Host Service, should enable resource management for Kubernetes containers - The proposed Cloud Bastion Host Service should allow passwords of resource accounts to be automatically changed. Customers can configure password change policies and specify when and how the policies work. A password change policy can be triggered manually, as scheduled, or periodically. Logs for password changes can be queried and downloaded. Resource accounts include the ones for host resources that have SSH, RDP, SMB, or Telnet enabled and accounts for database resources of many types such as MySQL, SQL Server, Oracle, PostgreSQL, GaussDB - The proposed Cloud Bastion Host Service should enable customers to configure account synchronization policies to let the system detect zombie accounts or unmanaged accounts in a timely manner - The proposed Cloud Bastion Host Service should allow Linux commands and Windows operations to be recorded by screen recordings. In this case, the idle duration in recordings can be filtered out and video recordings can be downloaded in just a few clicks - The proposed Cloud Bastion Host Service should support Centralized display of O&M statistics, including O&M action distribution over time, resource access times, session duration, command interception, number of commands, and number of transferred files. O&M reports can be exported in one click - The proposed Cloud Bastion Host Service should allow Two-person authorization, also called treasury mode. After two-person authorization is configured, O&M personnel can access core resources only after being authorized and authenticated by the administrator onsite

SL	Product Names/Items	Description of requirements
		- The proposed Cloud Bastion Host Service should enable System login-logs, resource login-logs, command execution-logs, file operation-logs, and two-person authorization logs to be remotely backed up to Syslog servers. System configuration-logs and session recording playback-logs can be remotely backed up to FTP or SFTP servers. - The proposed Cloud Bastion Host Service should enable customers to upload and download files via a browser, as well as share files from a Jump Server instance with the cloud servers it manages - The proposed Cloud Bastion Host Service should allow O&M engineers to log in to multiple authorized resources in one click. Moreover, multiple resources should be able to operate and maintain on the same browser tab page at the same time. Along with that, O&M engineers should be able to execute an O&M command for a group of resources concurrently - The proposed Cloud Bastion Host Service should allow O&M engineers to invite other engineers to join the same session for collaborative O&M and skill sharing - The proposed Cloud Bastion Host Service should enable scripts to be managed and edited in the Jump Server. Moreover, customers should be able to configure automated O&M tasks to let Jump Server automatically execute one or more preset O&M tasks, such as command execution, script execution, and file transfer tasks - The proposed Cloud Bastion Host Service should enable customers to apply for access and command authorization tickets. Moreover, customers should be able to obtain the resource control permissions by manually or automatically triggering a system ticket and submitting the ticket for approval - The proposed Cloud Bastion Host Service should enable customers to create custom approval processes. Along with that, multi-level approval, countersign approval, and multi-person approval should also be supported
6	Cloud Network Detection & Response (NDR) Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 1 Set of 10 GBP/s cloud software license of Cloud NDR Service - The proposed Cloud NDR Service should support heavy traffic detection and identification of typical application protocols, such as HTTP, TCP, UDP, DNS, SMTP, DHCP, FTP, MySQL, IMAP, SSH, SMB, RDP, Telnet, TLS, MSSQL, etc. - The proposed Cloud NDR Service should support identification and defense against typical attacks, such as brute force cracking, scanning, web attacks, web shells, reverse shells, malicious programs, abnormal connections, abnormal protocols, and data leakage - The proposed Cloud NDR Service should allow users to set the working mode, including the observation mode and interception mode - The proposed Cloud NDR Service should allow users to set blacklists and whitelists by IP address or IP address segment, and

SL	Product Names/Items	Description of requirements
		supports batch importing and exporting of blacklists and whitelists - The proposed Cloud NDR Service should support user access behavior audit, including middleware application access audit, high-risk protocol request connection audit, and hacker tool connection audit. The fields of behavior audit should include the time, risk level, alarm credibility, project ID, tenant name, rule ID, matched rule name, attack source IP address, attack source port, attacked IP address, attacked port, transmission protocol, application protocol, and direction - The proposed Cloud NDR Service should support rule signature engine, behavior analysis engine, machine learning engine, and authoritative third-party rule signature libraries, which can be uploaded offline at any time to improve the security detection rate and accuracy. - The proposed Cloud NDR Service should determine the source of attacks using the geographical location information library; loads offline update packages as required to access the most up-to-date intelligence, enabling swift analysis of attacks - The proposed Cloud NDR Service should provide visualizations of the global distribution of attackers, details of attack techniques, top attack sources, and the complete attack paths of individual attackers, including timelines, MITRE ATT&CK matrix representations, attack relationship Sankey diagrams, and in-depth attacker profiles. It should enable automatic or manual association of IP addresses to uncover common attack strategies and related attackers, and allow the downloading of PCAP files associated with attacks for comprehensive analysis - The proposed Cloud NDR Service should support north-south traffic detection at the Internet egress, cross-VPC traffic detection, and traffic detection between VMs on the same network segment in a VPC - The proposed Cloud NDR Service should provide detailed visualized security charts which displays key detection and response information in the entire attack defense process, including alarm response trend, total number of alarms, total number of detected alarms, number of attacked IP addresses, number of attacking IP addresses, alarm risk type distribution, alarm reliability distribution, alarm risk level distribution, alarm trend, top 5 attacker distribution, top 5 attack types, top 5 attacked IP addresses, and top 5 attackers (based on attacked IP addresses), number of attack responses, number of blocked attacks, number of blocked IP addresses, number of new whitelisted IP addresses, IP address status distribution, attack response distribution, blocking type distribution, attack response trend, distribution of top 5 blocked IP addresses, and top 5 blocked IP addresses. - The proposed Cloud NDR Service should allow users to view and search logs and attack alarms; provides IP address blocking and attack interception; and integrates developed graphical rule response system to respond to new threats within seconds. - The proposed Cloud NDR Service should support the search and analysis of traffic logs and attack logs and generates reports

SL	Product Names/Items	Description of requirements
		based on threat events, traffic statistics, and protocol statistics. Moreover, attack logs can display information such as the username, project ID, matched rule, quintuple, and attack payload of the attacked host.
7	Database Audit Service	- The proposed license should be seamlessly compatible and readily integrate-able with the existing cloud platform and should include at least 4 set of cloud software licenses (each set contains 5 Databases license) for Database Audit Security Service - The proposed database audit service should audit all operations (such as, insert, delete, update, and user-defined) on mainstream database systems in real time. The restoration operation information includes the session ID, database instance, database type, database user, client MAC address, database MAC address, client IP address, database IP address, client port, database port, client name, operation type, operation object type, response result, number of affected rows, start time, end time, SQL request statement, and request result fields. Agents can be installed for audit in CCE clusters. - The proposed database audit service should display the database audit information, including the device and host information of sessions and operation information - The proposed database audit service should display auditing information in multiple dimensions, such as session, statement, and behavior. Audit logs can be searched based on fields such as the client IP address, client name, database IP address, database user, operation type, rule name, and SQL statement keyword - The proposed database audit service should aggregate audit information of all managed databases across audit instances, including statement distribution, risk distribution, risk rule analysis, and session distribution, and displayed on the user interface - The proposed database audit service should provide report templates, including database security general report, database security compliance report, SOX report, database server analysis report, client IP address analysis report, DML command report, DDL command report, and DCL command report - The proposed database audit service should allow audit reports to be exported in PDF format -
8	Cloud Next Generation Firewall	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 5 cloud software licenses for Cloud Firewall Security Service. - The proposed cloud firewall should come with Access Control List (ACL) capability. Access control policies can be configured based on 5-tuple, address group, service group, and blacklist and whitelist. A protection rule contains at least the direction, source type, source address, destination type, destination address, service type, protocol type, source port, destination port, and IP location. For the blacklist and whitelist, you can set the address direction, IP address, port number, and protocol type. You can enter one or more IP addresses. A maximum of 100 IP addresses can be parsed at a time. Service groups can be configured and added by

SL	Product Names/Items	Description of requirements
		protocol, source port, and destination port. Pre-defined address groups and pre-defined service groups are supported. Traffic can be controlled based on 10+ application layer protocols - The proposed cloud firewall should support access control based on domain names or wildcard domain names. Users can add a domain name group of the website filtering type or DNS resolution type - The proposed cloud firewall should support access control over Internet border traffic, traffic between VPCs, and traffic between VPCs and Direct Connect gateways, as well as inbound and outbound traffic - The proposed cloud firewall should support intrusion prevention system (IPS), displays IPS signatures (attack type, severity, and impact scope), and supports the detection mode and block mode. Each IPS signature can be enabled and disabled. The blocking mode can be strict, moderate, or loose. Supports the antivirus function - The proposed cloud firewall should support virus defense, identifying and handling virus-infected files in traffic via HTTP, SMTP, POP3, FTP, IMAP4, and SMB protocols - The proposed cloud firewall should support proactive external connection analysis, proactively detects abnormal behaviors of cloud servers, collects external connection traffic statistics, and displays attack trends - The proposed cloud firewall should support the analysis of Internet-to-service access traffic, including Internet inbound and outbound traffic, attack trend, and top access IP addresses - The proposed cloud firewall should record intrusion event logs, traffic logs, and access control logs. Attack event logs include the occurrence time, attack type, risk level, rule ID, source IP address, source port, destination IP address, destination port, protocol, and application. Access control logs contain at least the receiving time, access source, source port, destination IP address, destination port, protocol, response action, and rule. Traffic logs contain at least the start/end time, access source, source port, destination IP address, destination port, protocol, number of stream bytes, and number of stream packets.
9	Cloud Native Application Performance Monitoring	- The proposed service should support collection of Kubernetes container logs, VM application logs, and IaaS system logs - The proposed service should support original log file viewing, real-time log refresh and search, and log file dumping - The proposed service should support log search by different criteria, context display, and search result export - The proposed service should support dashboard display and custom views of resource and application metrics - The proposed service should support common metrics, including disk, network, CPU, and memory metrics - The proposed service should support online upgrade, installation (including batch installation), and uninstall of Agent collectors - The proposed service should support rich metric calculation and aggregation; five statistical modes and multi-period data aggregation; component-level metric aggregation for queries

SL	Product Names/Items	Description of requirements
		- The proposed service should support threshold rules set for metrics such as resource usage, application status, and SLA metrics - The proposed service should support alarm viewing, clearance, filtering/search, and export - The proposed service should support Monitoring various types of data, covering JVM, JVMInfo, JavaMethod, URL, Exception, Tomcat, HTTPClient, MySQL, Redis, EsRestClient, Kafka, Netty, and gRPC metrics. - The proposed service should support automatic topology discovery and relationship generation, provides data trends, and displays a global topology. - The proposed service should support Supports non-intrusive tracing and trace search by trace ID and consumed time. Moreover, it should have Intelligent sampling: By default, error and slow requests are preferentially sampled, and fixed sampling policies such as Full Sampling, Percentage Sampling, and Fixed-Quantity Sampling are also supported. - The proposed service should allow users to directly view sampled log data on the trace page or go to the log system to view more details based on trace ID - The proposed service should support analysis of important URL links. - The proposed service should support application metric alarms, aggregation data alarms, alarms generated after metric data calculation, alarm automation, and large-scale alarm processing. - The proposed service should allow users to configure filter rules based on global, tenant, and environment tags, and filters and displays data based on rules. - The proposed service should monitor more metrics by using the metadata metric configuration model, and inherits configurations by application. Moreover, it should - support automatic adding of configurations. It means that middleware can be automatically discovered and monitored. - The proposed service should provide open APIs for third-party integration and custom scenarios. - The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least total 300 cloud software license for Application Operation and Performance Management.
10	Cloud Data Protection Service	- The proposed service should support the ability to automatically scan and sort data assets on the cloud, and display asset distribution on a map. - The proposed service should present a comprehensive view of cloud data assets, including asset overview, classification and grading statistics, risky asset statistics, attack information statistics, alarm/event handling statistics, and threat trends. - The service should be able to automatically associate with cloud data egresses to view all risky data egresses. - The solution should be able to automatically identify cloud data configuration risks based on cloud native assets. - The proposed service should allow data catalog information to be queried by service domain and data type.

SL	Product Names/Items	Description of requirements
		- The proposed service should allow customers to search for and filter data catalogs, view the details and relationships of the catalogs, and add categories and rating tags on the catalogs. - The proposed service should support various built-in classification and rating templates as well as custom classification based on the legal requirements of Bangladesh. - The proposed solution should also be able to enable, disable, modify, and delete algorithm rules for identifying different types of data. - The proposed solution shall support identifying sensitive data based on the combination of multiple conditions, such as regular expressions, keywords, column names, and column remarks. - The proposed service should support multiple data sources, including cloud-native object storage, cloud-native databases (MySQL, PostgreSQL, and SQL Server), cloud-native Hive, self-built MySQL, PostgreSQL, Oracle, TDSQL, SQL Server, and ElasticSearch. - The proposed service should support data of different types to be statically anonymized by means of hashing, masking, replacement, deletion, and rounding - The proposed service support watermarks to be added to and extracted from PDF, PPT, Word, and Excel files. - The proposed service should support adding watermarks to and extracting watermarks from images in *.jpg, *.jpeg, *.jpe and *.png formats. - The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 45 cloud software licenses for Data Security Center Service.
11	Integration with Existing Systems	Provide seamless integration including all necessary license as mentioned with existing eGov Cloud Platform in BCC NDC, ensuring compatibility with current infrastructure, workflows, and resource pools.
12	Reference Document	Performance and compliance reference documents related to the proposed solution should be included in the proposer's submission.
13	Warranty	The manufacturer's warranty must be specified, and a minimum warranty period of three (03) years should be offered for this solution starting from the date of commissioning.
14	Installation & Commissioning	Installation, testing, and commissioning must be carried out by the OEM, and the proposer is required to supply all necessary accessories needed for the installation and commissioning process.
15	Preferred: Scalability Requirements	• The solution must support modular and scalable infrastructure to accommodate future growth in data demands. • The architecture should enable seamless scaling of the following components:

SL	Product Names/Items	Description of requirements
		o Storage: Expansion of storage capacity in increments, up to at least 100% of the initial capacity without downtime or disruption to existing services. o Compute: Horizontal and vertical scaling of compute resources to meet future workload requirements. o Network: Support for increased bandwidth, additional virtual networks, and enhanced network throughput as required. • The platform must ensure compatibility with new hardware or software components for scaling purposes
16	Preferred: Future-Ready Features	• Software-Defined Infrastructure: The solution must leverage software-defined technologies (e.g., software-defined storage, networking) to facilitate dynamic resource allocation and easy integration of additional components. • Monitoring and Automation: Provide tools to monitor resource usage and automate scaling based on predefined thresholds.
17	Preferred: Energy Efficiency	• The proposed solution must align with energy efficient practices: o Equipment must comply with Energy Star® standards or equivalent certifications for energy efficiency. o Include options for dynamic power management to optimize power consumption based on workload.

SL. No. 11

Section VII – Purchaser's Requirements

D. Technology Specifications – Supply & Install Items

3.1 (B) Expansion of Capacity in existing Cloud Services

Page No: 146

As in issued RFP

B. Expansion of Capacity in existing Cloud Services

SL	Product Names/Items	Description of requirements
1	Computing Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 50 CPUs additional cloud software license for DC and 20 CPUs additional cloud software license for DR on the existing Private Cloud Platform of NDC. - All necessary relevant basic IaaS services along with necessary licenses shall be included with this including IMS, AS, VPC, ELB, EIP, VPN, ACL, SG, NAT Gateway, Direct Connect, DNS, Storage Service, etc.
2	Backup Service	The proposed solution should come with 700TB license for the expansion of existing Cloud Server Backup Service, this shall include both snapshot backup service and volume backup service.
3	Cloud Platform Operation & Management Requirements	- Necessary licenses should be offered for the O&M of the existing cloud platform and Cloud Management Portal. - Moreover, the proposed solution should come with necessary Operating System to deploy the distributed database and PostgreSQL
4	Integration with Existing Systems	Provide seamless integration including necessary licenses as mentioned with existing eGov Cloud Platform in BCC NDC, ensuring compatibility with current infrastructure, workflows, and resource pools.
5	Reference Document	Performance and compliance reference documents related to the proposed solution should be included in the proposer's submission.
6	Warranty	The manufacturer's warranty must be specified, and a minimum warranty period of three (03) years should be offered for this solution starting from the date of commissioning.
7	Installation & Commissioning	Installation, testing, and commissioning must be carried out by the OEM, and the proposer is required to supply all necessary accessories needed for the installation and commissioning process.

As Amended

C. Expansion of Capacity in existing Cloud Services

SL	Product Names/Items	Description of requirements
1	Computing Service	- The proposed license should be seamlessly compatible and readily integrable with the existing cloud platform and should include at least 30 CPUs additional cloud software license for DC and 20 CPUs additional cloud software license for DR on the existing Private Cloud Platform of NDC. - All necessary relevant basic IaaS services along with necessary licenses shall be included with this including IMS, AS, VPC, ELB, EIP, VPN, ACL, SG, NAT Gateway, Direct Connect, DNS, Storage Service, etc.
2	Backup Service	The proposed solution should come with 700TB license for the expansion of existing Cloud Server Backup Service, this shall include both snapshot backup service and volume backup service.
3	Cloud Platform Operation & Management Requirements	- Necessary licenses should be offered for the O&M of the existing cloud platform and Cloud Management Portal. - Moreover, the proposed solution should come with necessary Operating System to deploy the distributed database and PostgreSQL
4	Integration with Existing Systems	Provide seamless integration including necessary licenses as mentioned with existing eGov Cloud Platform in BCC NDC, ensuring compatibility with current infrastructure, workflows, and resource pools.
5	Reference Document	Performance and compliance reference documents related to the proposed solution should be included in the proposer's submission.
6	Warranty	The manufacturer's warranty must be specified, and a minimum warranty period of three (03) years should be offered for this solution starting from the date of commissioning.
7	Installation & Commissioning	Installation, testing, and commissioning must be carried out by the OEM, and the proposer is required to supply all necessary accessories needed for the installation and commissioning process.

SL. No. 12

Section VII – Purchaser's Requirements

Newly Added Items:

The Following Items have been added as per the Bangladesh Computer Council Feedback:

3.19 Security Servers for Data Exchange Platform (NRDEX) (Qty. 5 Nos)

SL	Product Names/Items	Description of requirements	Justification
1.	Brand Name	Any Internationally reputed Brand	Dedicated Physical Servers are considered for central/operator security servers of NRDEX under NDGIO/NDGIA, can be expanded in DSTAR based on demand. Can be installed in any location either in BDCCL or in BCC.
2.	Model	To be mentioned by the Bidder	
3.	Country of origin	To be mentioned by the Bidder	
4.	Country of Assemble	To be mentioned by the Bidder	
5.	Form Factor	2U Rack Server with Rack Mountable Rail Kit along with cable organization arm and Bezel Kit	
6.	Processor	Intel Xeon Scalable Gold with base frequency of 2.5 GHz or higher	
7.	Processor Generation	At least 5th Generation or higher	
8.	Number of Processors	2 (Two) Processor	
9.	Core per Processor	Minimum 32 core or higher	
10.	Cache Memory per processor	Minimum 60MB or higher	
11.	Chipset	Processor compatible latest generation Intel Chipset	
12.	Memory	- Minimum 32 DIMM slots per server - Minimum 16x64GB DDR5 Memory with advanced ECC capability	
13.	Graphics	- Integrated video card for standard configuration	
14.	Hard Drive	- Minimum 2 x 480GB SATA SSD - Minimum 6x7.68 TB NVMe flash disk.	
15.	Storage Array Controller	Should provide required RAID Controller Card supporting common RAID levels like 0,1,5,10 etc.	

SL	Product Names/Items	Description of requirements	Justification
16.	PCIe Expansion slots	Should support minimum 08 (Eight) or higher PCIe I/O expansion Slots	
17.	Network Interface Controller	- Minimum 1xDual 1Gb Copper NIC. - Minimum 2xDual 25GE Optical NIC - Minimum 4 x 10Gb SFP 28 Multimode transceiver.	
18.	Remote management port & features	Integrated remote management with following feature: - Must have RJ45 management port to remotely manage the server - Agentless out-of-band management - Integrated diagnostics and Power monitoring and reporting - Should support both HTML5 based web user interface and command line interface for management - Should support industry standard management protocols like IPMI v2 and SNMP v3 - Necessary license shall be activated from day 1 form out of band server management - Should support dual-mirror backup of firmware and support upgrading both primary and backup partitions at one time	
19.	Security Feature	- Must support UEFI secure boot - Must have Trusted Platform Module (TPM) - Must have chassis intrusion detection feature - System lock features	
20.	Power Supply &System Fan Support	Should have redundant power supply & hot-swappable fan modules	
21.	Operating System Support	Must support enterprise grade operating systems including Windows Server, RHEL, ESXi, SLES etc.	
22.	EOL/EOS Information	Offered product must not be End of Support (EoS) in 6 years (from the date of delivery)	
23.	Local Support	Must have local spare management service for smooth after sales support and service.	
24.	Compatibility	The Item must be compatible and integrate-able with the existing Cloud platform in BCC NDC.	
25.	Compliance	Must have CE, FCC, RoHS	
26.	Warranty & Support	Minimum 03 years comprehensive warranty from the date of commissioning with OEM 24x7x365 Global TAC support,	

SL	Product Names/Items	Description of requirements	Justification
		Patch & New Software Upgrade, RMA replacement. The RMA replacement must be within next business day (NBD).	
27.	Installation& Commissioning	Installation, testing and commissioning with necessary accessories	

3.20 Firewall for Data Exchange Interconnectivity (Qty. 2 Nos.)

SL	Product Names/Items	Description of requirements	Justification
1	Brand	Any Internationally reputed Brand	The firewalls are proposed for secure VPN interconnectivity between provider and consumer of data exchange platform to be placed along with the security servers.
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	Quality	The OEM of the Proposed brand must be in Niche or challenger or Leader quadrant in the latest Gartner Magic Quadrant for Network Firewall	
6	Enclosure Type	Rack Mountable, 1U	
7	Hardware Architecture	- The equipment must have minimum 240 GB local storage from day 1 - The equipment must have the capability to provide internal redundant power supplies available from day 1 - Interface requirements: Should have 8 x 1GE (COMBO) + 4 x 1GE (RJ45) + 10 x 10GE (SFP+) from day 1 and 6 x 10G SFP+ port equipped with 300m MM module from day 1 including patch cord	
8	Feature & Function Requirements	- Support concurrent SSL VPN users minimum 10000 and 5000 SSL VPN user from day 1 - Support Virtual firewalls minimum 2000 from day 1 - Firewall Throughput minimum 35 Gbps - Number of concurrent connections Minimum 20,000,000 - Number of new connections per second minimum 500,000 - IPSec VPN throughput minimum 30 Gbps - Threat Protection throughput minimum 7 Gbps - NGFW throughput minimum 8 Gbps - SSL VPN Throughput $\geq$ 3 Gbps - Security Policies minimum 150,000 - URL Filtering: minimum 130 Categories and minimum 500 million URLs	
9	Integrated Protection:	- The proposed equipment should support Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, anti-DDoS, URL filtering. - The proposed equipment should to provide a global configuration view, and manages policies in a unified manner.	

SL	Product Names/Items	Description of requirements	Justification
10	Application identification and control:	- The proposed equipment should Identifies over 6000 applications and supports the over 50 categories and over 20 risk labels for access control based on categories and labels. - The proposed equipment should support Application identification based on signatures, correlation, behaviors, user-defined - The proposed equipment should support SaaS application identification and access control based on signatures, DNS, IP addresses (IP address database of the top 50 SaaS applications), and first packets, and supports traffic steering based on SaaS applications	
11	Intrusion prevention and web protection	- The proposed equipment should support obtains the latest threat information in a timely manner and accurately detects and prevents vulnerability exploits - The proposed equipment should support coverage of tens of thousands of Common Vulnerabilities and Exposures. - The proposed equipment should support to detect malicious traffic, such as vulnerability attack traffic of common platform (such as Windows and Unix/Linux operating systems, databases, Apache, IIS, and Tomcat as well as middleware), web attack traffic (such as SQL injection, XSS, and RCE), botnets, remote control, and Trojan horses, and supports brute-force attack detection. - The proposed equipment should support minimum 25,000+ IPS signatures, and supports user defined signatures. - The proposed equipment should support attack forensics collection, full-flow packet obtaining and attack fragment display to facilitate O&M. - The proposed equipment should support User defined URL/host whitelist and blacklist - The proposed equipment should support Safe Search enforcement across five major search engines YouTube, Bing, Google, Yahoo, and Yandex, with mandatory filtering of illegal or inappropriate content in search results - The proposed equipment should support URL access controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors	

SL	Product Names/Items	Description of requirements	Justification
12	Anti-botnet	- The proposed equipment should support the detection and prevention of viruses and advanced malware, such as botnets, Trojan horses, worms, remote control tools, and spyware, and prevents the download of malware - The proposed equipment should support to quickly detects malicious traffic based on signatures, IP addresses, and domain reputation information	
13	Antivirus	- The proposed equipment should support to Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP 3 IMAP 4 NFS, and SMB - The proposed equipment should support to detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, crypto jacking software, and web shell programs - The proposed equipment should support virus detection for Office files, executable files (Windows/Linux/ script files, flash files, PDF files, RTF files, web pages, and images supports attack forensics collection - The proposed equipment should support the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip zip, rar and 7z - The proposed equipment should support multiple actions, such as alert, block, add declaration, and attachment deletion	
14	Advanced malware prevention	- The proposed equipment should uses detection technologies such as AI, semantic analysis, and Emulator, coupled with threat and reputation information, to detect packed malware, script morphing, and malware embedded in compound documents - The proposed equipment should support to send suspicious files to the local or cloud sandbox for further inspection to detect zero day malware	
15	Bandwidth management and Security policy management	- The proposed equipment should support managing per-IP bandwidth based on service application identification, Ensuring the network experience of key services and users. - The proposed equipment should support control methods include limiting the maximum bandwidth, guaranteeing the	

SL	Product Names/Items	Description of requirements	Justification
		minimum bandwidth, and changing the application forwarding priority. - The proposed equipment should support traffic management and control based on the VLAN ID, 5-tuple, security zone, region, application, and time range, and implements integrated content security inspection. - The proposed equipment should support policy self-learning, aggregates traffic matching a security policy, and generates more refined sub-security policies to achieve precise security management.	
16	DNS security	- The proposed equipment should support to detect malicious DNS requests, including C&C domain names, DGA generated domain names, compromised sites, and malicious domain names such as crypto jacking ransomware, and phishing domain names - The proposed equipment should have local malicious domain name database and supports support of 2 million malicious domain names in the local database.	
17	Uplink Selection	The proposed equipment should support service-specific PBR and intelligent uplink selection based on multiple load balancing algorithms (for example, based on bandwidth ratio and link health status) in multi-egress scenarios.	
18	VPN Encryption	The proposed equipment should support multiple highly available VPN features, such as IPsec VPN, SSL VPN and GRE.	
19	DLP and Mail Filtering	- The proposed equipment should support email address filtering, real time blacklist, and filtering by Multipurpose Internet Mail Extensions (header fields (such as sender, recipient, and subject), and restriction of the number of SMTP mails sent during a period of time - The proposed equipment should support identification of 100 real file types, user defined file name extensions, and file type-based upload/download control - The proposed equipment should support supports keyword filtering for Office documents, web pages, code, and TXT files - The proposed equipment should support user defined keywords, regular expressions, and weight configuration	

SL	Product Names/Items	Description of requirements	Justification
20	Security virtualization	The proposed equipment should support virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN. Users can separately conduct personal management on the same physical device.	
21	Server load balancing	The proposed equipment should support IPv6, Layer 4 /Layer 7 server load balancing, and multiple session persistence methods such as source IP address based and HTTP cookie based session persistence	
22	Routing	The proposed equipment should support multiple types of routing protocols and features, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.	
23	Deployment and reliability	The proposed equipment should support transparent, routing, tap, hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.	
24	User authentication	- The proposed equipment should support multiple authentication modes for Internet access users, including local Portal authentication and single sign-on (SSO). - The proposed equipment should support PPPoE client function to provide Internet access services, including user authentication and authorization and dynamic IP address allocation	
25	Operation & Maintenance and reporting	- The proposed equipment should support telemetry to automatically read information from hardware, such as fans, power modules, optical modules, Ethernet ports, temperature sensors, and drivers, and sends interface traffic statistics, CPU usage, and memory usage to the collector. - The proposed equipment should support to Provides reports, including traffic, threat, mail filtering, bandwidth management, system, policy matching, file blocking, data filtering, and URL filtering reports, and supports report customization and subscription - The proposed equipment should support Audits and regulates common user online behaviors, including FTP operations (download, and command), HTTP operations (search, and browsing), DNS,	

SL	Product Names/Items	Description of requirements	Justification
		Telnet, SNMP, and email sending and receiving operations - The proposed equipment should support to Serves as a proxy server for intranet terminals that have passed user authentication and security policy check to access the Internet (Supports HTTP and HTTPS). And also support to manage the online behaviors of users and send logs to the log server - The proposed equipment should have embedded network management system that offers a visualized and easy-to-use human-machine interface for network-wide visualization, one-click network-level service provisioning, and NE management. and also should have automatic network management capabilities, such as automatic deployment, diagnosis, and troubleshooting.	
26	Reference Document	Bidder should submit the required performance document and compliance reference document for the proposed device.	
27	Warranty	Minimum 3 (Three) years Manufacturer's warranty must be provided for this unit from the date of commissioning with OEM 24x7x365 Global TAC support, Patch & New Software Upgrade, RMA replacement. The OEM should have Depot in Bangladesh and the RMA replacement must be within next business day (NBD).	
28	Installation & Commissioning	Installation, testing and commissioning with necessary accessories	

3.21 Data Exchange Platform TOR and Interconnectivity Switch (Qty. 4 Nos.)

SL	Product Names/Items	Description of requirements	Justification
1	Brand	Internationally reputed Brand	The switches are proposed to use as serverfarm switch (qty. 2 Nos.) and to use as termination switch of WAN interconnectivity to establish secure VPN between provider and consumer of data exchange platform of NRDEX under NDGIO.
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	3rd Party Certification	Position of the OEM as Challenger or Leader quadrant in the 2025 Gartner Magic Quadrant for Data Center Switching will be preferred	
6	Enclosure Type	Rack mountable	
7	Hardware Architecture and Performance	- The equipment must have redundant Fan module AC Power Supply integrated from day one. - The proposed equipment must support switching capacity minimum 1.5Tbps. - The equipment must support forwarding performance minimum 900Mpps or more - The equipment airflow should be port-side intake	
8	Interface	- The equipment must have minimum 48 x 10G/1G fiber ports and 4 x 100G QSFP28 ports from day one. - Bidder must supply at least 24*10G Multi-mode SFP+ (0.1Km, LC) module and 12*1G single-mode SFP (10Km, LC) with necessary patch cord from day one and 04*100G QSFP28 (0.1Km, MPO) with 15 meters MPO-MPO cable from day one. The entire module must be from same OEM	
9	Switch Features	- Shall support Static, dynamic, and blackhole MAC address entries - Shall support source MAC addresses filtering - Shall support IPv4 multicast routes - Shall support ACL - Shall support M-LAG and must be equipped with 2-unit 100G QSFP28 High Speed Cable from day 1 for M-LAG - Shall support IPv4 and IPv6 FIB routes - Shall support minimum 4000 VRFs	

SL	Product Names/Items	Description of requirements	Justification
		- Shall support IPv4 dynamic routing protocols, such as RIP, OSPF, IS-IS, and BGP from day 1 - Shall support IPv6 dynamic routing protocols, such as RIPng, OSPFv3, IS-ISv6, and BGP4+ from day 1 - Shall support BFD for OSPF, BGP, IS-IS, and static route. - Shall support Hardware-based BFD - Shall support VRRP, VRRP load balancing, and BFD for VRRP. - Support Multicast routing protocols such as IGMP, PIM-SM - Shall support ERSPAN or similar - Support VXLAN and BGP EVPN from day 1 - Support RDMA and RoCE - Shall support SDN Features and can be integrated into mainstream SDN & cloud computing platforms - Must have support for integration with Ansible, Open stack Neutron or Open Programmability System (OPS) for automation - Shall have support to establish a non-blocking large Layer 2 network	
10	Security & QoS Features	- Shall support AAA, RADIUS and TACACS or similar authentication - Shall support defense against DoS attacks, ARP storms, and ICMP attacks - Shall support Port isolation, port security, and sticky MAC - Shall support Binding of the IP address, MAC address, port number, and VLAN ID - Shall support Traffic classification based on Layer 2, Layer 3, Layer 4, and priority information - Shall support STP with STP security features e.g. root guard/BPDU guard/filter etc.	
11	Management and Maintenance	- Shall have SNMPv1/v2c/v3 support - Shall have RMON, support Console, Telnet, and SSH terminals - Shall have internal logging including operation logs - Shall have Zero Touch Provisioning feature	

SL	Product Names/Items	Description of requirements	Justification
12	Reference Document	Bidder should submit the required performance document and compliance reference document for the proposed device.	
13	Warranty	Minimum 3 (Three) years Manufacturer's warranty must be provided for this unit from the date of commissioning with OEM 24x7x365 Global TAC support, Patch & New Software Upgrade, RMA replacement. The OEM should have Depot in Bangladesh and the RMA replacement must be within next business day (NBD).	
14	Installation & Commissioning	Installation, testing and commissioning with necessary accessories	

3.22 Advanced APT Detection with Malware Sandboxing (Qty. 1 Set)

SL	Product Names/Items	Description of requirements	Justification
1	Brand	To be mentioned by the bidder	Currently there are no enterprise grade malware analysis sandbox or simulation environment in National Data Center. The proposed solution will help NDC to verify file based malware coming into data center systems and cloud platform. Moreover, it will give manual analysis in controlled simulation environment to know the behavior of unknown malware. This will be also used by the government CIRT of NDC.
2	Model	To be mentioned by the bidder	
3	Country of Origin	To be mentioned by the bidder	
4	Country of Manufacturer	To be mentioned by the bidder	
5	System Architecture	The system must be inbuilt with OEM provided customized Physical Server with 3 node cluster including OS & Software and the server must be provided from day 1(one) with Dual power redundancy, necessary transceiver and patch cord	
6	Deployment Options	On-premises	
7	Performance	- The system must support Advanced threat detection throughput minimum 4 Gbps - The system must support Number of files inspected per day (dynamic analysis) minimum 100,000 - The system must support Number of files inspected per hour (static analysis) minimum 100,000	
8	Detection Capability	- The system should support simulation of multiple types of operating systems like Windows, Linux, and Android to dynamically detect threats in a virtual execution environment - The system should capable to provide multi-layer In-Depth Detection with 99% Accuracy or above - The system should support inspection of over 50 File Types for Comprehensive Detection of Unknown Malware - The system should support threat detection of Trojan horses, backdoors, worms, viruses, ransomware, adware, spyware, vulnerability exploits, grayware, hacker tools, phishing, and unknown threats. - The system should support comprehensive traffic restoration and detection - The system should capable of identifying all major file transfer protocols, such as HTTP, SMTP, POP3, IMAP, FTP and SMB, and	

		detecting malicious files transmitted using these protocols. - The system should capable to detect following types of file such as Compressed files (gz, rar, cab, 7zip, tar, bz2, zip), Windows PE (exe, dll, sys), Linux executable files (Elf, .o, .so), Android files (apk), Office 97-2003 (doc, xls,, ppt), Office 2007 and later (docm, dotx, dotm, xmsm, xmtx, xltm, xlam, pptm, potx, potm, ppsx, ppsm, ppam), RTF (rtf), Images (jpg, jpeg, png, tif, gif, bmp), WPS (wps, dt, dps), Web pages (htm, html, js), Flash (swf), JAVA (jar, class), PDF (pdf), Python (py, pyc, pyo), Executable scripts (cmd, bat, vbs, vbe, ruby, ps1, py) - The system should have built-in antivirus function to inspect preceding types of files, and CHM, ASP, PHP, COM, ELF files. - The system should support advanced threat protection in both IPv4 and IPv6 - The system should support AI / ML powered static code and executable code analysis on x86/ARM instruction sets.	
9	O&M Management	- The system should support Backup and restoration, panoramic monitoring, abnormal events detection, health check, and data collection - The system should support following file upload methods such as manual upload, upload by third parties, and upload by devices. - The system should support to upload files for inspection through OpenAPIs by Third-party users - The system should support sending logs to up to 10 external Syslogs servers simultaneously and support to send detection results to third-party users through Syslogs - The system should support sending Daily, weekly, and monthly reports to subscribed users specified email addresses. - The system should support sending alarm notifications through SMS messages and emails once high-risk malicious files are detected. - The system should support online, offline, and scheduled update of the detection engines and the signature database	
10	System security	- The system should support multi-tenant, workgroup-level domain-based management and operation log management. - The system should support password storage with encrypted format in configuration file to ensure Data Privacy	

11	Reliability	The system should support distributed clustering deployment. A single node fault should not affect system running. A cluster fault should not affect services on the live network.	
12	Deployment Mode	- The system should support interworking with firewalls and deploy in conjunction with NGFW/Firewall devices - The system should support deployment at the egress of the Internet, at the boundary of the data center	
13	Warranty & Subscription	- Minimum 3 (Three) years Manufacturer's warranty must be provided for this unit from the date of commissioning with OEM 24x7x365 Global TAC support, Patch & New Software Upgrade, RMA replacement. The OEM should have Depot in Bangladesh and the RMA replacement must be within next business day (NBD). - Minimum 3 (Three) years of Detection Capability Library Update Service with 3 years of Software upgrade support services	
14	Installation & Commissioning	- Installation, testing and commissioning with necessary accessories - Support Integration with existing firewall	

SL. No. 13

Section VII – Purchaser's Requirements

Page No: 54-55

As Per Issued/Published RFP:

1.1 **Subcontractors/vendors/manufacturers**

Subcontractors/vendors/manufacturers for major items of supply or services identified in the prequalification document must meet or continue to meet the minimum criteria specified therein for each item.

Subcontractors/vendors/manufacturers for the following additional major items of supply or services must meet the following minimum criteria, herein listed for that item:

Item No.	Description of Item	Minimum Criteria to be met
1.	Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)	• Must be operating in the local/ international market for five (5) years. • The product should have been implemented by Eight (8) customer / organization Note: A list of at least 8 customer/organization names where the product has been implemented. Supporting evidence for each listed implementation, such as: • Customer testimonials or reference letters.
2.	Core switch upgradation at DC (Qty. 02 Nos)	
3.	DC Service TOR Switch (Qty. 06 Nos)	
4.	DC Security Leaf Switch (Qty. 02 Nos)	
5.	DC BMS Gateway Switch (Qty. 02 Nos)	
6.	DC & DR Storage TOR Switch (Qty. 8 Nos)	
7.	DC & DR BMC TOR Switch (Qty. 04 Nos)	
8.	Hybrid- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	

9.	All- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	• Signed contracts or agreements • Case studies or deployment reports. • Any other official documentation proving implementation.
10.	All-Flash Production Storage for Cloud Platform at DR (Qty. 01 set)	
11.	Anti-Ransomware Backup Storage in DC (Qty. 01 Set)	
12.	DC Production Storage Upgradation (Qty. 1 Nos)	
13.	Backup Storage Upgradation for DC (Qty. 1 Nos)	
14.	DR Production Storage Upgradation (Qty. 1 Nos)	
15.	DC Computing Node Server (Qty. 30 Nos)	
16.	DC Security Node Server (QTY. 2 Nos)	
17.	DR Computing Node Server (Qty. 7 Nos)	
18.	IT Rack (Qty. 6 Nos)	
19.	Intelligent Smart PDU (Qty. 24 Nos)	

Failure to comply with this requirement will result in the rejection of the subcontractor/vendors/manufacturers.

As Amended

1.1 **Subcontractors/vendors/manufacturers**

Subcontractors/vendors/manufacturers for major items of supply or services identified in the prequalification document must meet or continue to meet the minimum criteria specified therein for each item.

Subcontractors/vendors/manufacturers for the following additional major items of supply or services must meet the following minimum criteria, herein listed for that item:

Item No.	Description of Item	Minimum Criteria to be met
1.	Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)	• Must be operating in the local/ international market for five (5) years. • The product should have been implemented by Eight (8) customer / organization Note: A list of at least 8 customer/organization names where the product has been implemented. Supporting evidence for each listed implementation, such as: • Customer testimonials or reference letters. • Signed contracts or agreements • Case studies or deployment reports. • Any other official documentation proving implementation.
2.	Core switch upgradation at DC (Qty. 02 Nos)	
3.	DC Service TOR Switch (Qty. 06 Nos)	
4.	DC Security Leaf Switch (Qty. 02 Nos)	
5.	DC BMS Gateway Switch (Qty. 02 Nos)	
6.	DC & DR Storage TOR Switch (Qty. 8 Nos)	
7.	DC & DR BMC TOR Switch (Qty. 04 Nos)	
8.	Hybrid- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	
9.	All- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	
10.	All-Flash Production Storage for Cloud Platform at DR (Qty. 01 set)	

11.	Anti-Ransomware Backup Storage in DC (Qty. 01 Set)	
12.	DC Production Storage Upgradation (Qty. 1 Nos)	
13.	Backup Storage Upgradation for DC (Qty. 1 Nos)	
14.	DR Production Storage Upgradation (Qty. 1 Nos)	
15.	DC Computing Node Server (Qty. 20 Nos)	
16.	DC Security Node Server (QTY. 2 Nos)	
17.	DR Computing Node Server (Qty. 7 Nos)	
18.	Intelligent Smart PDU (Qty. 100 Nos)	
19.	Security Servers for Data Exchange Platform (NRDEX) (Qty. 5 Nos)	
20.	Firewall for Data Exchange Interconnectivity (Qty. 2 Nos.)	
21.	Data Exchange Platform TOR and Interconnectivity Switch (Qty. 4 Nos.)	
22.	Advanced APT Detection with Malware Sandboxing (Qty. 1 Set)	

Failure to comply with this requirement will result in the rejection of the subcontractor/vendors/manufacturers.

SL. No. 14

Section VII – Purchaser's Requirements

As Per Issued/Published RFP

Page No: 186-188

A. IMPLEMENTATION SCHEDULE TABLE

The implementation part of assignment mentioned in this Request for Proposals must be completed within 18 (eighteen) weeks from the date of effective of the contract. Detailed technical designs and relevant documentation must be provided including physical, logical and service oriented layout designs, etc. Roles and responsibilities of all stakeholders regarding the activities and services must be provided in detail with clear separation of duties.

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
0	Project Plan	N/A	NDC, ICT Tower	W2	-	W3	No
1	Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
2	Core switch upgradation at DC (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
3	DC Service TOR Switch (Qty. 06 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
4	DC Security Leaf Switch (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
5	DC BMS Gateway Switch (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
6	DC & DR Storage TOR Switch (Qty. 8 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
7	DC & DR BMC TOR Switch (Qty. 04 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
8	Hybrid- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
9	All- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
10	All-Flash Production Storage for Cloud Platform at DR (Qty. 01 set)	N/A	NDC, ICT Tower	W08	W10	W11	No
11	Anti-Ransomware Backup Storage in DC (Qty. 01 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
12	DC Production Storage Upgradation (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
13	Backup Storage Upgradation for DC (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
14	DR Production Storage Upgradation (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
15	DC Computing Node Server (Qty. 30 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
16	DC Security Node Server (QTY. 2 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
17	DR Computing Node Server (Qty. 7 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
18	IT Rack (Qty. 6 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
19	Intelligent Smart PDU (Qty. 24 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
20	Training and delivery of documentations	N/A	NDC, ICT Tower	W3	N/A	W16	No

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
21	Operational Acceptance of the System	N/A	NDC, ICT Tower	W16	N/A	W18	Operational Acceptance

As Amended

A. IMPLEMENTATION SCHEDULE TABLE

The implementation part of assignment mentioned in this Request for Proposals must be completed within 18 (eighteen) weeks from the date of effective of the contract. Detailed technical designs and relevant documentation must be provided including physical, logical and service oriented layout designs, etc. Roles and responsibilities of all stakeholders regarding the activities and services must be provided in detail with clear separation of duties.

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
0	Project Plan	N/A	NDC, ICT Tower	W2	-	W3	No
1	Expansion of Existing Private Cloud Platform Software (DC & DR, QTY. 01 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
2	Core switch upgradation at DC (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
3	DC Service TOR Switch (Qty. 06 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
4	DC Security Leaf Switch (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
5	DC BMS Gateway Switch (Qty. 02 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
6	DC & DR Storage TOR Switch (Qty. 8 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
7	DC & DR BMC TOR Switch (Qty. 04 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
8	Hybrid- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
9	All- Flash Production Storage for Cloud Platform at DC (Qty. 1 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
10	All-Flash Production Storage for Cloud Platform at DR (Qty. 01 set)	N/A	NDC, ICT Tower	W08	W10	W11	No
11	Anti-Ransomware Backup Storage in DC (Qty. 01 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No
12	DC Production Storage Upgradation (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
13	Backup Storage Upgradation for DC (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
14	DR Production Storage Upgradation (Qty. 1 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
15	DC Computing Node Server (Qty. 20 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
16	DC Security Node Server (QTY. 2 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
17	DR Computing Node Server (Qty. 7 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
18	Intelligent Smart PDU (Qty. 100 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
19	Security Servers for Data Exchange Platform (NRDEX) (Qty. 5 Nos)	N/A	NDC, ICT Tower	W08	W10	W11	No
20	Firewall for Data Exchange Interconnectivity (Qty. 2 Nos.)	N/A	NDC, ICT Tower	W08	W10	W11	No
21	Data Exchange Platform TOR and Interconnectivity Switch (Qty. 4 Nos.)	N/A	NDC, ICT Tower	W08	W10	W11	No
22	Advanced APT Detection with Malware Sandboxing (Qty. 1 Set)	N/A	NDC, ICT Tower	W08	W10	W11	No

Line Item No.	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
23	Training and delivery of documentations	N/A	NDC, ICT Tower	W3	N/A	W16	No
24	Operational Acceptance of the System	N/A	NDC, ICT Tower	W16	N/A	W18	Operational Acceptance

SL. No. 15

Section VII – Purchaser's Requirements

As Per Issued/Published RFP
Page No: 192-193

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS)

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1.	Expansion of Existing Private Cloud Platform Software (DC & DR)	3.1	3rd floor, ICT Tower	01 Set
2.	Core switch upgradation at DC	3.2	3rd floor, ICT Tower	2 Nos
3.	DC Service TOR Switch	3.3	3rd floor, ICT Tower	6 Nos
4.	DC Security Leaf Switch	3.4	3rd floor, ICT Tower	2 Nos
5.	DC BMS Gateway Switch	3.5	3rd floor, ICT Tower	2 Nos
6.	DC & DR Storage TOR Switch	3.6	3rd floor, ICT Tower	8 Nos
7.	DC & DR BMC TOR Switch	3.7	3rd floor, ICT Tower	4 Nos
8.	Hybrid- Flash Production Storage for Cloud Platform at DC	3.8	3rd floor, ICT Tower	01 Set

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
9.	All- Flash Production Storage for Cloud Platform at DC	3.9	3rd floor, ICT Tower	01 Set
10.	All-Flash Production Storage for Cloud Platform at DR	3.10	3rd floor, ICT Tower	01 Set
11.	Anti-Ransomware Backup Storage in DC	3.11	3rd floor, ICT Tower	01 Set
12.	DC Production Storage Upgradation	3.12	3rd floor, ICT Tower	01 Nos
13.	Backup Storage Upgradation for DC	3.13	3rd floor, ICT Tower	01 Nos
14.	DR Production Storage Upgradation	3.14	3rd floor, ICT Tower	01 Nos
15.	DC Computing Node Server	3.15	3rd floor, ICT Tower	30 Nos
16.	DC Security Node Server	3.16	3rd floor, ICT Tower	02 Nos
17.	DR Computing Node Server	3.17	3rd floor, ICT Tower	07 Nos
18.	IT Rack	3.18	3rd floor, ICT Tower	06 Nos
19.	Intelligent Smart PDU	3.19	3rd floor, ICT Tower	24 Nos
20.	Warranty	-	3rd floor, ICT Tower	Three (3) for Years from the date of Operational Acceptance

As Amended

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS)

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1.	Expansion of Existing Private Cloud Platform Software (DC & DR)	3.1	3rd floor, ICT Tower	01 Set
2.	Core switch upgradation at DC	3.2	3rd floor, ICT Tower	2 Nos
3.	DC Service TOR Switch	3.3	3rd floor, ICT Tower	6 Nos
4.	DC Security Leaf Switch	3.4	3rd floor, ICT Tower	2 Nos
5.	DC BMS Gateway Switch	3.5	3rd floor, ICT Tower	2 Nos
6.	DC & DR Storage TOR Switch	3.6	3rd floor, ICT Tower	8 Nos
7.	DC & DR BMC TOR Switch	3.7	3rd floor, ICT Tower	4 Nos
8.	Hybrid- Flash Production Storage for Cloud Platform at DC	3.8	3rd floor, ICT Tower	01 Set
9.	All- Flash Production Storage for Cloud Platform at DC	3.9	3rd floor, ICT Tower	01 Set

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
10.	All-Flash Production Storage for Cloud Platform at DR	3.10	3rd floor, ICT Tower	01 Set
11.	Anti-Ransomware Backup Storage in DC	3.11	3rd floor, ICT Tower	01 Set
12.	DC Production Storage Upgradation	3.12	3rd floor, ICT Tower	01 Nos
13.	Backup Storage Upgradation for DC	3.13	3rd floor, ICT Tower	01 Nos
14.	DR Production Storage Upgradation	3.14	3rd floor, ICT Tower	01 Nos
15.	DC Computing Node Server	3.15	3rd floor, ICT Tower	20 Nos
16.	DC Security Node Server	3.16	3rd floor, ICT Tower	02 Nos
17.	DR Computing Node Server	3.17	3rd floor, ICT Tower	07 Nos
18.	Intelligent Smart PDU	3.18	3rd floor, ICT Tower	100 Nos
19.	Security Servers for Data Exchange Platform (NRDEX)	3.19	3rd floor, ICT Tower	05 Nos
20.	Firewall for Data Exchange Interconnectivity	3.20	3rd floor, ICT Tower	02 Nos
21.	Data Exchange Platform TOR and Interconnectivity Switch	3.21	3rd floor, ICT Tower	04 Nos
22.	Advanced APT Detection with Malware Sandboxing	3.22	3rd floor, ICT Tower	1 Set

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
23.	Warranty	-	3rd floor, ICT Tower	Three (3) for Years from the date of Operational Acceptance

All other terms and conditions of RFP No: EDGE-G1B shall remain unchanged. This Addendum No. 1 shall be considered **an integral part** of the RFP document and shall be binding on all proposers who have obtained the RFP document from the Purchaser in accordance with ITP 6.3.

(Dr. Md. Taibur Rahman)
Project Director (Joint Secretary)
Enhancing Digital Government and Economy (EDGE)Project
Bangladesh Computer Council (BCC), ICT Division.