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-3-5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh
Phone: +880241001721 Fax: +88-02-55006791, E-mail: piu.edge@bcc.gov.bd, www.bcc.gov.bd

Memo No.: 56.01.0000.046.07.083.25-164 Date: 06 August 2025

Minutes of Pre-Proposal Meeting

Contract title: Supply, Installation and Commissioning of National Security Operation Centre (NSOC)

Request For Proposals No: EDGE-G20

Date and Time: 16 June 2025, 11.00 a.m.

Venue: Conference Room of EDGE Project.

The meeting commenced with a welcome note from the Project Director, Enhancing Digital Government and Economy (EDGE) Project, who greeted all participants (see *Attachment-1* for list of attendees) and requested the Deputy Project Director to proceed.

The Deputy Project Director highlighted the key Purchaser Requirements, Procurement Milestones, Evaluation Process, and applicable Procurement Regulations to be followed during the RFP process. Members of the Procurement and Technical Team further elaborated on the specific requirements for this procurement.

The meeting emphasized adherence to procurement timelines, submission deadlines, and evaluation procedures as per the RFP. The ITP Clause 17 of RFP Document for Proposal Price was also discussed in the meeting.

Participants were informed that a **Rated Criteria** approach will be used to evaluate the non-price (technical) aspects of the proposals. The **techno-commercial evaluation** will follow the below weightage:

- **Technical Proposal:** 40%
- **Financial Proposal:** 60%

Assessment Steps (as per ITP 32.1 of RFP) of Technical Evaluation:

Step 1 – Initial Compliance Check:

Only those proposals that meet the **Purchaser's Technical Requirements** (as detailed in Section VII of the RFP) will proceed with detailed technical evaluation.

Step 2 – Rated Criteria Evaluation (as per PDS ITP 32.2 of RFP):

The technical evaluation will assign scores based on the following criteria, which collectively constitute 100% of the technical evaluation score (equivalent to 40% of the total proposal evaluation):

Sl.No.	Technical Factor	Weight in percentage (Weight in %)	Reference
1	Preliminary Project Plan addressing the required topics.	20%	Section IV – Proposal Forms, Format of the Technical Proposal
2	Cyber security management strategies and implementation plans	10%	Section IV – Proposal Forms, Format of the Technical Proposal
3	**Preferred:** EASM Feature	10%	Section VII – Purchaser's Requirements, 3.7 Detailed Technical Specifications and Requirements,

Enhancing Digital Government & Economy Project
BCC
ICT Division

			3.7.27 External Attack Surface Management, Serial Number 14.
4	**Preferred:** Malware Analysis Sandbox	10%	Section VII – Purchaser's Requirements, 3.7 Detailed Technical Specifications and Requirements, 3.7.28 Malware Analysis Sandbox (On-premise), Serial Number 13:
5	Security Information and Event Management (SIEM) **Preferred:** Gartner Magic Quadrant-Based Product Evaluation	25%	Section VII – Purchaser's Requirements, 3.7 Detailed Technical Specifications and Requirements, 3.7.1 Security Information and Event Management (SIEM), Serial Number 16:
6	Privileged Access Management (PAM) **Preferred:** Gartner Magic Quadrant-Based Product Evaluation	25%	Section VII – Purchaser's Requirements, 3.7 Detailed Technical Specifications and Requirements, 3.7.3 Privileged Access Management (PAM), Serial Number 18
	Total	**100%**	

The detailed scoring methodology is provided in **Section III – Evaluation and Qualification Criteria** of the RFP.

Participants were reminded to submit their queries (if any) within 14 days of RFP publication. As of the date of this meeting, no queries were received via email or in person.

The Project Director opened the floor for questions. Queries raised during the meeting were noted for formal response. Participants were requested to submit any additional queries by 17 June 2025. The procuring entity will issue a written response in due time.

There being no further questions, the meeting concluded with a vote of thanks from the Project Director.

Attachments:

- Attachment-1: List of Participants
- Attachment-2: Queries & Responses

Dr. Md. Taibur Rahman
Project Director (Joint Secretary)

Enhancing Digital Government & Economy Project * BCC ICT Division

Memo No.: 56.01.0000.046.07.083.25-164 Date: 06 August 2025

Copy forwarded for kind information & necessary action with request to acknowledge receipt in writing within 2 days:

1..

....

2. Office Copy

Dr. Md. Taibur Rahman
Project Director (Joint Secretary)

Attachment -1

Attendance Sheet

Enhancing Digital Government and Economy (EDGE)
Bangladesh Computer Council (BCC)
Information And Communication Technology Division (ICTD)
Ministry Of Posts, Telecommunications and Information Technology
Youth Tower (Level-3, 4 and 5), Plot # 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh
Phone: +880241001721, Fax: +880255006791, E-Mail: pd.edge@bcc.gov.bd, Website: www.bcc.gov.bd

Attendance Sheet (Firms Representative)

Pre-Proposal Conference

Contract Title: National Security Operation Center (NSOC) for NCSA & BCC

Package No: EDGE-G20

Date & Time: 16 June 2025 at 11:00 Bangladesh Time (BST=GMT +6:00 hours)

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
01	Sumaiya Khanom Manager	Thakral Information Systems Pvt. Ltd.	01730091391 sumaiya.khanom@thakral-bd.com	
02	Mohammad Masud Manager, Sales	Thakral Information Systems pvt. Ltd.	01730091379 mohammad.masud@thakral-bd.com	
03	Emran Hossain A. SR. Manager	Omega Exim Limited	01721613213 Emran.Hossain@omegaeximltd.com	
04	Azadur Rahman	BG interactive ltd.	0191437-2485 azad@bg-interactive.com	
05	Nafis Ehtisham Executive Director	BG Interactive Limited	01733503157	

8

Enhancing Digital Government & Economy Project * BCC ICT Division

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
06	A.H. Mahbool Ullah	Star Computer Systems Limited.	01711083958 mahboolullah@stargroup-bd.com	
07	Reazul Islam Chief Operating Officer.	ADN Technologies.	01841093270 reaz@adntechnologies.net	
08	Abdullah Executive	Synesis IT Ltd	01911592527 rakibul.islam@synesisit.com.bd	
09	Md. Nazrul Islam Director, Business FSN solutions	FSN Solutions	01700744694 nazrul@fsnitsolutions.com	Nazrul
10	Md. Monirul Islam Bhuiyan. Sales Dist	Smart Data Technologies Ltd	01713064506 monirul@smartdataltd.com	M.
11	Shahanaj Begum	FSN Solution Ltd	01716011098 shahanaj@fsnitsolutions.com	
15	Shahana Abdin	FSN solutions	(516) 849-7414 shahana@fsnitsolutions.com	
16	Lutfe Habib Khan	Global Brand PLC	01717457660 lutfe_khan@globalbrand.com.bd	

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
17	AREF MAHMOOD CTO	ADNT	01713036306 aref@adntechnology.net	
18	Md mamun-ar-Rashid ~~CSL~~ GM, Promt Sales	CSL Technologies Ltd	01842464154 mamunrashid@csltechltd.com	
19	Md. Emdadul Haque AGM, ~~CSL~~ Pre Sales	CSL Technologies Ltd.	01712161393 emdad@csltechltd.com	
20	Abdullah Al Noman Public sector Lead	Microsoft	01685695033 v-anoman@microsoft.com	
21	Farzana Afrin Tisha Tech Lead	Microsoft	01726542885 v-ftisha@microsoft.com	
22	Jahirul Islam PreSales Engr.	Trustaira	01678170021 jahirul.islam@trustaira.com	
23	MD. AHSANUL HAQUE Sr. Technical Account Manager	Trustaira	01713115878 ahsanul.haque@trustaira.com	
24	TAUKIR AHMED Key Accountmanger	Trusteir	01936913941 taukir.ahmed@trusteir.com	

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
25	Md. Waheduzzaman AGM	Global Brand PLC	01711965443 md_waheduzzaman@globalbrand.com.bd.	
26	Musbah Ahmed Mahdi Manager	SmartData Technologies Ltd.	01716588708 mahdi@smartdataltd.com	
27	Mushfique Bin Hossain Executive	BG Interactive LTD.	01753167395 ~~musf~~ mushfique@agilemindscorp.com	
28	Kw Nusrat Zirat Khushbu	China shandong Hi-speed Qianfang Tech. co. LTd	01963045994 sdhscitfoBangladesh@gmail.com	Khushbu
29	Hasin Iqbal Sadi	Cisco	01710992212 hassadi@cisco.com	
30	Jamil Uddin Bhuiyan Cyber Security Specialist	Cisco	01711080074 jabhuiya@cisco.com	
31	Mehadi Hasan	Am square Limited	01686139150 ovihasa@amsquaregroup.com	
32	Maung Tan	Smart Technologies(BD) Ltd	01313002183 maung.tan@smartbd.com	

Enhancing Digital Government & Economy Project • BCC ICT Division

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
33	S. K. Bhattacharya General Manager	Smart Technologies	01713245294 shewarjan@smarttd.com	
34	SWAPAN Sr. Manager	Link³ Technologies Ltd	01787667405 swapan.roy@link3.net	
35	Sanjit Chandra Das	Selopia	01841637242	
36	Md. Ferdous Rubaiat Hossain	Fusion Net Ltd.	01552388160 info@fusionbd.net	
37	Al Imran chowdhury	Link3 Tech	01849377315 imran.chowdhury@link3.net	
38	Shaikhul Islam Sr. Executive	Star Computer System Limited	01601483244 shayok@stargroup-bd.com	
39	Vincent Solution Artect	Whale Cloud	01704361299 chen.jianjun113@iwhalecloud.com	
40	Uttam Consultant	whale cloud.	1.0740631506 iconiuttam@gmail.com	

8

Enhancing Digital Government & Economy Project * BCC ICT Division

SL	Name & Designation	Name of the Proposer/ Organization	Contact (Cell & Email)	Signature
~~06~~ 41	Md. Ekramul Kabeer Country Manager	Ingram Micro	01611582212 mdekramul.kabeer @ingrammicro.com	
~~07~~ 42	Md. Borhan Hafiz Manager, Business Development	FSIT Solution Ltd.	01602058896 borhan@fsit solutions.com	
08				
09				
10				

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Attachment-2

Responses of Queries for Supply, Installation and Commissioning of National Security Operation Centre (NSOC) (Contract Package # EDGE-G20)

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
1	I3.7.6 Next Generation Firewall for SOC 8 Performance Requirement	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 10 Gbps enterprise mix throughput from single appliance - Minimum 6 Gbps Threat protection throughput from single appliance - Minimum 500,000 concurrent sessions per seconds - Minimum 4K VLANs	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 10 Gbps enterprise mix Firewall throughput from single appliance - Minimum 6 Gbps Threat protection throughput from single appliance - Minimum 500,000 concurrent sessions per seconds - Minimum 4K VLANs Remarks: Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	Yes, the term enterprise mix throughput refers to the overall firewall throughput performance under typical enterprise traffic conditions, including a mix of protocols such as TCP, UDP, HTTP, HTTPS, and others.
2	3.7.7 VPN Firewall for CII Integration 8 Performance Requirement	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 20 Gbps enterprise mix throughput from single appliance - Minimum 15 Gbps Threat protection	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 20 Gbps enterprise mix Firewall throughput from single appliance - Minimum 15 Gbps Threat protection	Yes, the term enterprise mix throughput refers to the overall Firewall Throughput under typical enterprise traffic conditions, which includes a combination of protocols such as TCP, UDP, HTTP, HTTPS, etc.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
		throughput from single appliance - Minimum 1 million concurrent sessions per seconds - Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 - Minimum 4K VLANs	throughput from single appliance - Minimum 1 million concurrent sessions per seconds - Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 - Minimum 4K VLANs Remarks: Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	
3	3.7.10 Server Farm Switch 5 Interface	- Minimum 4x10 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port	- Minimum 4x100 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port Remarks: Please clarify, is the uplink requirements is correct or typo mistake, usualy all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	Bidder can propose higher but it should be 10G compatible. The original specification of "Minimum 4x10 GE uplink ports" is intentional and not a typographical error. The requirement was defined based on the current core network architecture and bandwidth demands at the site, where 10G uplinks are sufficient to meet performance and scalability needs.

Enhancing Digital Government & Economy Project * ICT Division BCC

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
				However, to accommodate advancements in hardware and vendor flexibility, bidders are allowed to propose uplink ports of higher capacity (e.g., 40G or 100G), provided that the solution ensures full backward compatibility with 10G speeds. This approach ensures interoperability with the existing infrastructure while allowing the use of higher-capacity equipment if available.
4	3.7.10 Server Farm Switch 13 Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - DoS attack defense - ARP attack defense, and - ICMP attack defense	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like	The mentioned features such as Spanning Tree Port Fast, Root Guard, and others are to indicate the expected functionality and protection mechanisms, not to mandate any vendor-specific proprietary terms. Bidder may offer equivalent standard protocols or features that deliver the same

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	or higher level of functionality and protection. Bidder must clearly mention the proposed equivalent features in their technical documentation during bid submission for proper evaluation.
5	3.7.12 Perimeter Switch for CII Integration 5 Interface	- Minimum 4x10 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port	- Minimum 4x100 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port Remarks: Please clarify, is the uplink requirements is correct or typo mistake, usualy all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	The uplink port requirement mentioned as Minimum 4 x 10GE uplink ports is correct and intentional based on the intended use case and network design for specific layers or roles of the equipment (e.g., access or TOR switches). However, for higher capacity network layers such as core or aggregation, the requirement specifies Minimum 4 x 100GE uplink ports, which is also intentional and in line with expected performance standards. Bidder can propose higher but it should be 10G compatible.

2 8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
6	3.7.12 Perimeter Switch for CII Integration 13 Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - DoS attack defense - ARP attack defense, and - ICMP attack defense	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Bidders can implement these features using proprietary names or mechanisms, provided that the proposed solution complies with industry-standard protocols and delivers equivalent or superior functionality as specified. Therefore, Bidder are allowed to propose equivalent or higher functionality features according to different terminologies.
7	3.7.13 Access Switch for SOC Room and Management 13 Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and	Bidder can implement these features using proprietary names or mechanisms, provided that the proposed solution complies with industry-standard protocols and delivers equivalent or superior functionality as specified. Therefore, Bidder are allowed to propose equivalent or higher functionality features

8

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			supports Root Protection which is similar to Root Guard	according to different terminologies.
8	3.7.13 Access Switch for SOC Room and Management 15 Management	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow or Similar Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality	Refer to Addendum No.47 of RFP Document.
9	1.3.2 Average Annual Turnover	Minimum average annual turnover of US$ 4.0 million or equivalent amount, calculated as total certified payments received for contracts in progress or completed, in best three (3) within the last five (5) years from the Proposal submission date	Could you please clarify whether the minimum average annual turnover of US$ 4.0 million should be demonstrated by the lead bidder alone, or if the combined turnover of consortium members or joint venture partners can be considered to meet this criteria?	Please refer to Qualification Criteria 1.3.2 of Section III – Evaluation and Qualification Criteria of RFP Document, which specifies the requirement for Annual Turnover. In the case of a Joint Venture (JV), all members combined must meet the total requirement. Additionally, each JV member must individually meet at least 25% of the requirement, and at least one member must meet a minimum of 40% of the requirement.

Digital Government & Economy Enhancing Project ★
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
10	1.4.2 Specific Experience	"Participation as a prime supplier, management contractor, JV5 member, sub-contractor, with a minimum contract value US$ 3.0 million or equivalent amount under maximum two (2) similar contract(s) within the last five (5) years prior to the proposal submission deadline, that have been successfully and substantially completed and that are similar to the proposed Information System. The contract will be treated as similar, if it includes any of the following components: Enterprise Security Tools (such as SIEM, SOAR, EASM), Enterprise Computing Hardware (e.g., servers, switches, firewalls, storage), Large-Scale Enterprise Software (e.g. Virtualization Software, ITSM), or any combination thereof, as described in Section VII Purchaser's Requirements for SOC/Network Operations Centers (NOC)/ Data Center (DC)/ Disaster Recovery (DR). The successfully completed similar contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s).	The proposer must have participated in up to two similar contracts, each worth at least USD 3 million within the past five years—does this experience need to be local, or are international projects also acceptable?	Please refer to Qualification Criteria 1.4.2 of Section III – Evaluation and Qualification Criteria of RFP Document, which outlines the requirement for Specific Experience. Relevant experience from successfully completed contracts whether local or international projects is considered acceptable.

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
		The successful supply completion certificate issued by the Proposer's parent/subsidiary/sister/affiliate firm will not be considered for specific experience."		
11	148 3.7.1 (SIEM)		The tender specifies multi-tenant, scalable architecture. Could you clarify preferred hypervisor and minimum hardware configuration per node?	Please refer to RFP hardware Technical Specification, Architecture will be design Based on the below available hardware & virtualization software. 3.7.14 Virtualization Software 3.7.15 Physical Servers for On-Premise SOC Tools 3.7.18 FC Storage
12	148 3.7.1 (SIEM)		Will separate clusters be required for divisions, or a single multi-tenant architecture is acceptable?	single multi-tenant architecture is required however multiple cluster accepted as per load.
13	150 3.7.1 (SIEM)		The AI/ML component must baseline without human intervention. Could you clarify the expected baseline period (weeks, months)?	Shall be customizable in range of 2-4 Weeks
14	153 3.7.2 (SOAR)		Are there a minimum number of pre-built playbooks you expect on day-1 delivery?	A minimum of 10 pre-built playbooks on day-1 delivery, covering common use cases such as malware detection,

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
				phishing response, user account anomalies, data exfiltration, and privilege escalation. Bidders shall specify the number and type of pre-built playbooks provided by the OEM as part of their proposal. Additional custom playbook development capabilities should also be supported.
15	153 3.7.2 (SOAR)		Will there be separate roles for designing and executing the playbooks in your operations team?	Yes
16	155 3.7.3 (PAM)		Are there specific platforms or OSs we must prioritize first (Linux, Windows, routers, databases)?	As per the standard PAM feature support, the system must support privileged access management across all major enterprise operating systems, including Windows, Linux, and Unix-based platforms. Also, the solution should support integration with network devices, databases, cloud environments, and virtualization platforms to ensure comprehensive and centralized management of privileged accounts across the organization..

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
17	163 3.7.4 (EDR)		Are there CPU or memory utilization limits we should account for on endpoints?	As low as possible
18	163 3.7.4 (EDR)		Do you have a preferred OS mix (percentage Windows vs Linux)?	There is no preferred OS mix. The solution supports all major operating systems including Windows, Linux, and macOS and is designed to detect and respond to threats across these platforms. It also integrates well with network devices, databases, and other enterprise systems to ensure wide coverage.
19	186 3.7.9 (NBA/Sandbox)		Are there minimum throughput or latency criteria we should account for when designing the solution?	Please refer to RFP 3.7.9 Network Behavior Analysis (NBA) with Sandboxing, Serial number: 4
20	186 3.7.9 (NBA/Sandbox)		Will all suspicious files and flows be routed to the sandbox, or policy controls will select samples?	Shall be configurable to choose between the options.

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
21	N/A Security, Reporting, Integration		Are there preferred API standards or protocols we should be compliant with (like STIX/TAXII, CEF, Webhooks)?	Bidder are allowed to propose equivalent or higher as per industry standard protocol compliance.
22	N/A Support & Licensing		Could you clarify baseline license dimensions (EPS, endpoints, analysts)?	Refer to Addendum No. 1 of RFP Document. EPS: 3.7.1 Security Information and Event Management (SIEM), SL:12, Page: 152 EDR: 3.7.4 Endpoint Detection and Response (EDR), SL:19, Page: 170 Analyst:3.7.2 Security Orchestration, Automation, and Response (SOAR), SL: 10, Page: 154
23	N/A Support & Licensing		Do you require remote service, or a local support engineer 24x7?	Please refer to SLA in RFP

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
24	N/A Support		What service level agreements (SLAs) do you expect for incident response and hardware replacement if something fails?	Please refer to RFP Priority Level 1: Emergency/Urgent/Critical Business Impact
25	N/A Licensing		How many endpoints, network devices, and privileged accounts should we license for EDR, PAM, and SIEM respectively?	Please refer to RFP
26	Page , 3.7.1 Security Information and Event Management (SIEM) (Solution Type)	On premise Self-hosted	Public Cloud Justification for Change: To effectively support the onboarding of 34 Critical Information Infrastructures (CIIs), Bangladesh's national SOC should adopt a cloud-based platform instead of on-premises technology, as it offers **scalable architecture, real-time access to global threat intelligence, and built-in AI/ML capabilities for advanced threat detection and automated response—ensuring faster deployment, lower total cost of ownership, and future-proofing against evolving cyber threats.** **Scalability for 34 CII's:** Cloud-native SOCs offer elastic scalability to onboard all 34 CII without hardware limitations or performance bottlenecks. **Built-in AI & ML Capabilities:** Cloud platforms provide advanced AI/ML for real-time threat detection, behavioral analytics, and automated incident response—	Public Cloud Not Permitted. On premise Self-hosted. As per draft of Personal Data Protection Ordinance-2025 (PDPO), any government confidential data can not be cross border

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			capabilities that are cant be replicated to on-prem. **Access to Global Threat Intelligence:** Cloud SOCs integrate with global threat intelligence feeds, enabling faster detection of emerging threats, including zero-day and nation-state attacks which onprem technology cant provide. **Faster Deployment & Lower TCO:** Cloud solutions reduce time-to-deploy from months to weeks and eliminate CapEx on infrastructure, offering a more cost-effective and agile model. **High Availability & Resilience:** Cloud platforms offer built-in redundancy, disaster recovery, and 24/7 uptime—critical for national-level cyber defense- double investment would required for site-wise redundency, disester recovery **Compliance & Security Standards:** Leading cloud SOCs are certified for global standards (ISO 27001, SOC 3, GDPR, etc.), ensuring compliance with both international and local regulations. **Future-Proof Architecture:** Cloud platforms evolve continuously with new features, integrations, and threat models, ensuring long-term adaptability and innovation.	
27	Page 147, 3.7.1 Security Information and Event	The proposed SIEM solution shall meet the standard (PCI DSS, ISO 27001,	SOC 1, SOC 2, SOC 3 – Service Organization Controls HIPAA – U.S. healthcare data protection	Refer to Addendum No. 16.

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
	Management (SIEM) (Security and Compliance)	NIST CSF etc.) and out-of-box compliance.	ISO/IEC 27001, 27017, 27018 – Information security and cloud privacy Justification for Change: SOC, PCI DSS, ISO, IEC certifications are critical in selecting products for a national SOC because they ensure compliance, security assurance, operational readiness, and vendor accountability—essential for protecting national infrastructure and citizen data. **Complying with SOC 1, SOC 2, SOC 3, HIPAA, ISO/IEC 27017, and 27018 alongside PCI DSS, ISO 27001, and NIST CSF strengthens SIEM solution security**. It broadens compliance scope to cloud readiness, healthcare privacy, and service reliability. This approach meets multiple regulatory demands, ensures data protection, robust audit trails, and trust. Business justification emphasizes risk mitigation, governance, and operational excellence. Extended standards support cloud and hybrid models, secure vendor services, advanced encryption, threat intelligence, and compliance transparency. It positions NSOC to handle diverse data types confidently, ensuring comprehensive controls, excellent service delivery, and readiness for evolving threats.	
28	Page 148, 3.7.1 Security Information and Event	"The supplier can offer any flexible and scalable licensing model based on the following baseline information:	"Log Ingestion Breakdown Timeline as Follows- A. 3 month EPS size	Refer to Addendum No. 18.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
	Management (SIEM) (Licensing Option)	Log Data Volume: 1500+ GB/day EPS: 40,000 or unlimited EPS Retention: 30 days before archival Redundancy factor: 1 - Unlimited log sources and EPS value "	B. 6 months EPS size C. 9 months EPS size D. 18 months EPS size E. 26 months EPS size F. 36 months EPS size Retention Analytics Log- suggest to keep 90 days" Justification for Change: The current specification of 1,500 GB/day log ingestion **from day one is unrealistic**, as log volume will gradually increase over time with the phased onboarding of all CIIs—a process expected to span several years. To ensure cost-effectiveness and operational realism, we propose a month-wise log ingestion model, aligned with the actual onboarding timeline. This phased approach avoids overprovisioning and ensures optimal resource utilization. Additionally, setting the analytics log retention period to 90 days strikes the right balance between: Effective threat detection and forensic investigation Trend analysis and compliance Storage efficiency and cost control This revised model ensures the National SOC remains agile, scalable, and sustainable, while meeting evolving security	

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			demands without compromising performance or budget	
29	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for SIEM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as SIEM solution from Gartner's Leader Quadrant can ensures the followings: **Proven reliability, scalability, and compliance** with global standards **Superior threat detection, analytics, and governance capabilities**—critical for national-level SOC operations **High customer satisfaction, continuous innovation, and long-term vendor support** In contrast, Visionary quadrant solutions, while innovative, **may lack the operational maturity, integration readiness, and proven scalability** required for a national SOC. These solutions often carry higher implementation risks and may not meet the stringent demands of national cybersecurity infrastructure.	Refer to Addendum No. 19.
30	Page 154, 3.7.2 Security Orchestration,	On premise	Public Cloud Justification for Changes:	Public Cloud Not Permitted. On premise.

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
	Automation, and Response (SOAR) (Deployment Option)		**SOAR capabilities must be cloud-native** to ensure real-time access to AI/ML engines, which are essential for automating threat detection, response workflows, and data protection at national scale. Cloud-based SOAR platforms offer **built-in automation, adaptive playbooks, and continuous learning models**, enabling faster and more intelligent incident response. In contrast, **on-premises SOAR solutions often lack real-time AI/ML integration**, limiting their ability to adapt to evolving threats and automate complex workflows effectively. This shift ensures the NSOC remains **agile, intelligent, and future-ready,** while reducing operational complexity and enhancing national cyber resilience.	As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.
31	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (Licensing Option)	On premise license for 50 analysts from day and shall be scalable in the future	Suggesting to have unlimited licences for SOC analyst which can extended to CII's as if required Justification for Changes: **Scalable CII Onboarding:** An unlimited SOAR license allows the NSOC to assign access to CIIs as needed, without being constrained by license limits—supporting flexible, phased onboarding across all 34 CIIs.	Refer to Addendum No. 21

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			Future-Proofing Operations: A limited license model would restrict automation capabilities as the platform scales, potentially delaying incident response and increasing operational risk over time. **Unified Licensing for SIEM + SOAR + UEBA:** Bundling these core components under a single license model ensures: - Cost efficiency through simplified procurement and predictable budgeting - Operational agility with seamless integration and centralized management - Simplified governance and compliance tracking across the entire security stack **Strategic Value:** Unlimited licensing ensures the NSOC remains agile, scalable, and responsive to evolving national cybersecurity needs—without the administrative burden or cost spikes of license expansion.	
32	Page 149, 3.7.3 Privileged Access Management (PAM) (NA)		Identity and Access Management (IAM) is the foundational /1st layer of any Security Operations Center (SOC) including with the capabilities of Privileged Access Management (PAM). Justification for Changes: Identity and Access Management **(IAM) is foundational** to SOC operations, managing all user identities and access—while PAM	IAM is out of scope of current RFP. However bidder can integrate PAM with Open Source IAM of their choice if needed

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			only secures privileged accounts. **PAM without IAM lacks context**, making it ineffective for enforcing least privilege or detecting identity-based threats. Including **IAM ensures centralized identity governance, supports Zero Trust architecture,** and enables scalable, secure onboarding of CIIs. A **combined IAM + PAM approach enhances visibility, compliance, and operational efficiency,** making it essential for a national SOC.	
33	Page 149, 3.7.3 Privileged Access Management (PAM) (License)	The proposed solution should be offered for 50 admin user license with unlimited device support for 3 years	The proposed solution should be offered for 50 user IAM including PAM license for 3 years Justification for Changes:	As per the RFP, the proposed solution must include 50 user licenses covering both IAM and PAM functionalities for a duration of 3 years, with unlimited device support. While an open-source IAM solution is within the scope of this RFP, the bidder must ensure that the integrated solution delivers full functional compliance without imposing additional licensing costs on the purchaser. To eliminate ambiguity, bidders are requested to clearly define their licensing model specifying user roles,

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
				categories (e.g., admin users, service accounts), and any concurrency or usage limitations to ensure accurate commercial comparison during evaluation.
34	Page 149, 3.7.3 Privileged Access Management (PAM) (Deployment)	Bidder must provide installation and implement high availability in Active-Active mode and solution should be on-premise appliance or VM based deployment	Bidder must provide solutions in Cloud with high-availability, redundancy, 99.9% uptime Justification for Changes: As outlined in section 3.7.3, the Identity and Access Management (IAM) solution, including (PAM), should be deployed as a cloud-based platform. The deployment must ensure high availability, redundancy, and a minimum uptime SLA of 99.9%, to meet the reliability and resilience requirements of a national-scale SOC	Not permitted in public cloud. As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.
35	Page 149, 3.7.3 Privileged Access Management (PAM) (General features)	Solution must be from leaders quadrant of Gartner report for PAM	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for IAM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as IAM solution from Gartner's Leader Quadrant can ensures the followings: Gartner Leaders offer **proven, end-to-end IAM capabilities with operational**	Refer to Addendum No. 1 of RFP Document.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
			maturity, scalability, and integration readiness—essential for a national SOC while Visionary vendors, often lack the depth, stability, and full feature set needed to deliver a complete, secure, and compliant IAM solution at scale. Selecting a **Leader ensures lower risk, better support, and long-term value, aligning with the NSOC's** mission for resilience, compliance, and operational excellence.	
36	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (NA)		The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for EDR published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as EDR solution from Gartner's Leader Quadrant can ensures the followings: **Gartner Leaders** offer **proven, scalable, and fully integrated EDR capabilities**, essential for national-level threat detection and response while Visionary vendors often **lack the maturity, reliability, and ecosystem integration** needed for a complete and secure deployment. Choosing a **Leader ensures lower risk, better support, and long-term value,** aligning with the NSOC's mission for resilience, compliance, and operational excellence.	Refer to Addendum No. 1 of RFP Document.

8

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
37	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (General requirement)	The proposed solution should be on premises solution but will protect all type of server (physical, virtual, cloud) from a single console.	The proposed solution should be Cloud agnostic but will protect all type of users, servers, applications (physical, virtual, cloud) from a single console. Justification for Changes: We are recommending NSOC to follow the Cyber Ordinance 2025 Act 5(Cha) guidance while building national SOC. “এই অধ্যাদেশের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অন্যালিসিস এর নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুশন (যেমন – Security Information & ইভেন্ট ম্যানেজমেন্ট-SIEM, Security Orchestration, Automation, and Response-SOAR, Endpoint Detection and Response - EDR)/Extended Detection and Response - XDR, Network Detection and Response - NDR , ইত্যাদি) ব্যবহার এবং লগ আদান প্রদানের উদ্যোগ গ্রহণ “	Public Cloud Not Permitted. On premise. As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.
38	3.7.10-3.7.15, 3.7.18 & 3.7.19 Server Farm Switch (Qty. 4) FC Switch (Qty. 02) Perimeter Switch for CII Integration (Qty. 2) Access Switch for SOC Room and Management (Qty. 2) Virtualization Software Physical Servers for on premise SOC tools (Qty. 8)		NOT REQUIRED: Cloud solutions doesn’t required any of these hardware components Justification for Changes: “Recommendation to Remove On-Premise Hardware: In light of the proposed shift to cloud-based solutions, we also recommend removing the associated on-premises hardware requirements that were originally intended	Public Cloud Not Permitted. As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
	FC Storage (Qty. 01) 42U Server Rack (Qty. 02)		to support on-premises requirement. Cloud solutions will ensure required hardware capacity from the Cloud itself without incurring any additional cost to NSOC"	
39	Page 152, 3.7.28 Malware Analysis Sandbox (On-premise) (Deployment Option)	On premise	Public Cloud Justification for Changes: Cloud-based solutions, delivered as SaaS, eliminate the need for baseline installation and instead require only configuration to onboard servers and users from CIIs. Unlike fixed on-premise setups, cloud platforms offer elastic compute power to handle high-volume data, real-time threat intelligence updates, and seamless integration with SIEM and SOAR. This approach reduces hardware maintenance, accelerates threat analysis, enhances global accessibility and disaster recovery, and supports continuous automation, centralized management, and rapid deployment of new detection techniques—making it the most agile, efficient, and future-ready model for NSOC operations.	Public Cloud Not Permitted. As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	Purchaser Response
40	Page 152, 3.7.31 Installation & Implementation of NSOC System (Scope of Work)	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Storage, Servers, Switches, Workstations, Video Wall, Surveillance Systems, and related infrastructure.	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Workstations, Video Wall, Surveillance Systems, and related infrastructure. Justification for Changes: "To establish a truly modern and future-ready Security Operations Center (SOC) for the government, it is essential to incorporate several additional components that are currently missing from the existing plan. We would be pleased to offer complimentary consultancy services to help identify and design the most suitable cloud-based SOC architecture. Our approach includes recommending a multi-tenant model, where each government agency operates within its own secure and isolated tenant. This structure empowers agencies with greater autonomy to manage their infrastructure while maintaining centralized oversight and collaboration with the ICT National SOC team. We are confident that this model will enhance operational efficiency, scalability, and security across all participating agencies."	Public Cloud Not Permitted As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border. In this regard Issued RFP clause "Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Storage, Servers, Switches, Workstations, Video Wall, Surveillance Systems, and related infrastructure." Remain same.

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
41	**3.7.1** **SIEM** **Section 3.7.1: Gartner Magic Quadrant Positioning for SIEM**		In Section 3.7.1, there appears to be a discrepancy between Question 13 and Question 16 regarding acceptable Gartner Magic Quadrant positions for the proposed SIEM solution. Question 13 states that the solution “”shall be positioned either in the Leader or Visionaries quadrant of the latest Gartner Magic Quadrant for SIEM published in 2024””, suggesting a strict compliance requirement. However, Question 16 outlines a scoring mechanism where products in the Challenger quadrant are eligible for partial points. Could you please clarify whether a solution positioned as a Challenger in the 2024 Gartner Magic Quadrant for SIEM would be considered compliant under Question 13, or would it be disqualified regardless of scoring eligibility under Question 16?”	Refer to Addendum No. 20.
42	**3.7.29 / 3.7.33.1** **“Section 3.7.29 and Section 3.7.33.1: SOC Training and Analyst Responsibilities**		Section 3.7.29 refers to SOC Trainings (with Certification Exams), while Section 3.7.33.1 states that the supplier shall provide full-time operational and maintenance personnel (including analysts) during the SLA period.	Ans 1: SOC training only for the client’s internal team. Ans 2: supplier is providing full-time SOC analysts as per

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			We would appreciate clarification on the following points: 1. Who is expected to receive the SOC training? Is it intended for the client's internal team, the supplier's analysts, or both? 2. If the supplier is providing full-time SOC analysts as per the SLA, who will be responsible for actively monitoring the environment the client's team (post-training) or the supplier's analysts? 3. Could you please clarify the expected capacity and role division between trained personnel and the supplied analysts during operations?"	the SLA, For actively monitoring the environment the client's team & also from supplier's analysts are responsible. Ans 3: Refer to RFB 3.7.33.1 Operational and Maintenance Personnel during SLA.
43		What are the applicable VAT and Tax percentages for the following components: • Hardware • Software • Implementation, Training & Maintenance • Annual Maintenance Contract (AMC)		Please refer to Clause 17 of the Instructions to Proposers (ITP) under Part 1 – Request for Proposal Procedures of the RFP Document, which provides guidance on the preparation of the Financial Proposal by the Proposer.

Enhancing Digital Government & Economy Project * BCC ICT Division

44	Reference: Page 152, Serial 12 – Licensing Options (EPS Based)		The RFP mentions support for up to 40,000 Events Per Second (EPS), while also referencing "unlimited EPS licensing." For pricing purposes, we require clarification: Should we consider 40,000 EPS as the baseline for our licensing and pricing quotation? The term "unlimited EPS" introduces ambiguity in estimating costs, especially since our solution is priced based on EPS tiers. Kindly confirm the expected EPS volume for initial deployment to enable accurate cost estimation.	Refer to Addendum No. 18
45	Reference: Page 182, Serial 142 – NSOC Infrastructure Scope		The RFP indicates a minimum of 200 monitored hosts under the NSOC infrastructure. As our licensing model is per IP/host-based rather than slab-based, we seek clarification on the following: May we consider 200 monitored hosts as the basis for our initial pricing calculation? Alternatively, should we project and quote for a higher number of hosts expected during future scaling?	Should provide a minimum of 200 but should have option to scalability.
46			What baseline datasets or behavioral patterns should AI/UEBA modules initially learn from? Are any sample log repositories or synthetic data to be provided?	The AI/UEBA modules should initially learn from baseline datasets that reflect typical user and entity behavior across the organization, including authentication logs, access patterns, privilege usage, and network activity. If available, sample log repositories or anonymized historical

Enhancing Digital Government & Economy Project
BCC
ICT Division

				data from the organization will be used to accelerate model training. In the absence of such data, the system can be bootstrapped using synthetic data and refined over time as real-time behavior is observed post-deployment.
47			Is there any Integration of existing Platform/ Product/ Service required? If yes, which platforms?	NSOC tools platform/product/service will be integrated with each other.
48			How is tenant separation expected to be enforced — logically (e.g., namespace isolation) or physically (e.g., separate VMs)?	Logically
49			Does the Ministry have specific use cases or threat models (e.g., nation-state APTs, insider threats) that vendors should demonstrate?	The Ministry doesn't have specific use cases or threat models.
50			Will the Ministry provide detailed specifications of the target data center(s) e.g., rack space, power per rack, HVAC capacity?	Please Refer to RFP Hardware Technical Specification
51			What are the runtime and load expectations for UPS systems (in kVA and minutes)? Will backup diesel generators be available on-site?	It's responsibility of client to ensure passive infrastructure uptime.
52			Will the Ministry provide detailed specs of existing hardware in NDC to ensure full compatibility during sizing and integration?	Yes. Will be provided during the implementation period.

53			Could you kindly provide the floor and furniture layout of the NSOC room?	Please sign the NDA to do the site survey for layout.
54	**3.7.6 Next Generation Firewall for SOC 8 171 Performance Requirement**	The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 10 Gbps enterprise mix throughput from single appliance - Minimum 6 Gbps Threat protection throughput from single appliance - Minimum 500,000 concurrent sessions per seconds - Minimum 4K VLANs	Change to The firewall shall support at least 5 virtual firewall instance from day 1 -Minimum 10 Gbps enterprise mix Firewall throughput from single appliance -Minimum 6 Gbps Threat protection throughput from single appliance -Minimum 500,000 concurrent sessions per seconds -Minimum 4K VLANs Remarks Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	Please refer query response number 1.
55	**3.7.7 VPN Firewall for CII Integration 8 175 Performance Requirement**	The firewall shall support at least 5 virtual firewall instance from day 1 -Minimum 20 Gbps enterprise mix throughput from single appliance -Minimum 15 Gbps Threat protection throughput from single appliance -Minimum 1 million concurrent sessions per seconds -Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 -Minimum 4K VLANs	Change To The firewall shall support at least 5 virtual firewall instance from day 1 -Minimum 20 Gbps enterprise mix Firewall throughput from single appliance -Minimum 15 Gbps Threat protection throughput from single appliance -Minimum 1 million concurrent sessions per seconds -Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 -Minimum 4K VLANs Remarks Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	Please refer query response number 2.

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

56	**3.7.10 Server Farm Switch 5 188 Interface**	Minimum 4x10 GE uplink Ports -Minimum 48x10/25 GE SFP downlink Ports -1 Out of Band Management Port	Minimum 4x100 GE uplink Ports -Minimum 48x10/25 GE SFP downlink Ports -1 Out of Band Management Port RemarksPlease clarify, is the uplink requirements is correct or typo mistake, usually all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	Please refer query response number 3.
57	**3.7.10 Server Farm Switch 13 188 Switch Security Feature**	Spanning Tree Port Fast Root Guard Storm control (multicast and broadcast) Linklevel flow control (IEEE 802.3x) The proposed equipment should support CPU defense DoS attack defense ARP attack defense, and ICMP attack defense	Spanning Tree Port Fast or Similar Root Guard or Similar Storm control (multicast and broadcast) Linklevel flow control (IEEE 802.3x) The proposed equipment should support CPU defense ARP attack defense, and ICMP attack defense Remarks Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edgedport which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Please refer query response number 4.
58	3.7.12 Perimeter Switch for CII Integration 5 190 Interface	Minimum 4x10 GE uplink Ports Minimum 48x10/25 GE SFP downlink Ports 1 Out of Band Management Por	Minimum 4x100 GE uplink Ports Minimum 48x10/25 GE SFP downlink Ports 1 Out of Band Management Port Remarks Please clarify, is the uplink requirements is correct or typo mistake, usualy all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	Please refer query response number 5.
59	3.7.12 Perimeter Switch for CII	Spanning Tree Port Fast Root Guard Storm control (multicast and broadcast) Linklevel flow control	Spanning Tree Port Fast or Similar Root Guard or Similar Storm control (multicast and	Please refer query response number 6.

BCC ICT Division
Enhancing Digital Government & Economy Project

	Integration 13 191 Switch Security Feature	(IEEE 802.3x) The proposed equipment should support CPU defense DoS attack defense ARP attack defense, and ICMP attack defense	broadcast) Linklevel flow control (IEEE 802.3x) The proposed equipment should support CPU defense ARP attack defense, and ICMP attack defense Remarks Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edgedport which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	
60	3.7.13 Access Switch for SOC Room and Management 13 193 Switch Security Feature	Spanning Tree Port Fast Root Guard Storm control (multicast and broadcast) Linklevel flow control (IEEE 802.3x) The proposed equipment should support CPU defense ARP attack defense, and ICMP attack defense	Spanning Tree Port Fast or Similar Root Guard or Similar Storm control (multicast and broadcast) Linklevel flow control (IEEE 802.3x) The proposed equipment should support CPU defense ARP attack defense, and ICMP attack defense Remarks Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edgedport which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Please refer query response number 7.
61	3.7.13 Access Switch for SOC Room 15 192 Management	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow or Similar Remarks	Please refer query response number 8.

Enhancing Digital Government & Economy Project * BCC ICT Division

8

			Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality	
62	3.7.9: Network Behavior Analysis (NBA) with Sandboxing 7 187 Sandbox Environment	The solution shall ensure process, registry, file system, network connection, and memory manipulation monitoring with API call analysis.	Please Remove Remarks As per our observation it is related to EDR/XDR solution features. Not related to NBA Solution. Request to delete these features.	Refer to Addendum No. 45. .
63	**3.7.8 Ticketing, IT Service, IT Asset & NMS System 48 178 Analyst Module**	Clone/Copy Ticket with unique ticket number & editable field of new ticket	Manual ticket creation with copy/paste of relevant info; unique ticket number autogenerated; all fields editable Remarks In alignment with ITIL best practices, it is generally recommended to track one issue or request per ticket. This approach promotes clear accountability, accurate reporting, and effective resolution management. Allowing ticket cloning can introduce risks such as data duplication, fragmented information, and potential confusion in ticket tracking. Therefore, to maintain data integrity and process clarity, the practice of manually creating new tickets—while referencing relevant information from previous tickets—is preferred	Both manual and open ticket from existing by cloning can be preferred.
64	3.7.8 Ticketing, IT Service, IT Asset & NMS System 200 185 NMS Module	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drilldown capabilities.	should allow multiple network maps to be nested with drill down capabilities. Remarks	Refer to Addendum No. 43.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			Background customization is not available and its OEM Specific.	
65	3.7.8 Ticketing, IT Service, IT Asset & NMS System 201 185 NMS Module	The proposed monitoring solution able to add interfaces as a component in a map to monitor the availability of interface/VLANs.	The proposed monitoring solution must be able to monitor the availability and performance of interfaces/VLANs per device, and provide visibility through status indicators, alerts, and drilldown dashboards. Visual representation on topology maps should include devices, with interface/VLANlevel metrics accessible through the device view Remarks While the intent is to ensure visibility into the health and availability of network interfaces and VLANs, displaying individual interfaces or VLANs as separate visual components on a topology map is not a standard industry practice. Most advanced NMS platforms are designed to: Represent devices as map components Display interface and VLANlevel health/status data within the device context Trigger interfacelevel alerts, performance graphs, and reports Provide drilldown visibility into all monitored interfaces/VLANs on a perdevice basis This approach reduces visual clutter on topology maps and improves clarity and manageability of largescale networks.	Refer to Addendum No.1 of RFP Document
66	3.7.1 Security Information and Event Management (SIEM) 5 148 Log Collection or Ingestion Capabilities	The proposed solution shall support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture with a 3rd party packet capture solution where required.	Reuest to remove "full packet capture with a 3rd party packet capture solution where required" Remarks	Refer to Addendum No. 9.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			Full Packet Capture is not part of SIEM solution	
67	3.7.4 Endpoint Detection and Response (EDR) 9 165 Threat Intelligence Integration	The EDR should allow for custom IOC import and management (SHA1, SHA256 hashes, IP addresses, domains, URLs, YARA rules).	Request to change as "The EDR should allow for custom IOC import and management (SHA1, SHA256 hashes, IP addresses, domains, URLs, YARA rules) through Threat intel Feed coonector supported STIX/TAXII feed"	Bidders are encouraged to detail the available mechanisms for IOC import and management, including integration with Threat Intelligence Feeds. The solution must support open standards for threat intelligence sharing, such as STIX/TAXII or equivalent, to ensure interoperability and alignment with industry best practices.
68	3.7.4 Endpoint Detection and Response (EDR) 10 165 False Positive Management	The solution should provide tools for exception management with approval workflows.	Request to change as "The solution should provide tools for exception management"	Refer to Addendum No. 29.
69	3.7.4 Endpoint Detection and Response (EDR) 11 166 Response and Remediation Capabilities	The solution must provide rollback capabilities for automated actions when appropriate.	Request to change as "The solution must support reversing persistent changes and restoring the system to its previous state"	No change, because the request and clause are same.
70	3.7.4 Endpoint Detection and Response (EDR) 11 166 Response and	The solution must support live response capabilities with minimal latency (<5 seconds).	Request to change as "The solution must support live response capabilities with minimal latency"	Refer to Addendum No. 32

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Remediation Capabilities			
71	3.7.4 Endpoint Detection and Response (EDR) 11 166 Response and Remediation Capabilities	The solution must enable system remediation actions including forced logoff, restart, or shutdown.	Request to change as "The solution must enable system remediation actions including Terminate process, Delete file, Clean persistent data, Block address on Firewall"	Refer to Addendum No.1 of RFP Document
72	3.7.4 Endpoint Detection and Response (EDR) 14 168 Data Management and Compliance	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	Request to change as "The EDR should include features or integrated with other tool like SIEM for compliance with HIPAA, PCI DSS, and other relevant regulations."	Refer to Addendum No.1 of RFP Document
73	3.7.6 Next Generation Firewall for SOC (Qty. 02) 11 173 Next Generation Firewall Security Features	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high priority websites.	Request to change as "The firewall should provide a URL category database with over 240 million URLs and accelerates access to specific categories of websites, improving access experience of high priority websites."	Refer to Addendum No.1 of RFP Document
74	3.7.6 Next Generation Firewall for SOC (Qty. 02) 15 174 Warranty and Maintenance	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 3 (three) business days.	?	Not Agreed
75	3.7.7 VPN Firewall for CII Integration (Qty.	The firewall should provide a URL category database with over 400 million URLs and	Request to change as "The firewall should provide a URL category database with over 240 million	Refer to Addendum No.1 of RFP Document

BCC ICT Division Enhancing Digital Government and Economy Project

	02) 11 176 Next Generation Firewall Security Features	accelerates access to specific categories of websites, improving access experience of high priority websites.	URLs and accelerates access to specific categories of websites, improving access experience of high priority websites."	
76	3.7.7 VPN Firewall for CII Integration (Qty. 02) 15 177 Warranty and Maintenance	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 3 (three) business days.	?	Not Agreed
77	3.0.1 Network Behavior Analysis (NBA) with Sandboxing 7 187 Sandbox Environment	The solution shall ensure process, registry, file system, network connection, and memory manipulation monitoring with API call analysis.	This is SIEM features and request to remove the line.	Refer to Addendum No. 45
78	3.0.1 Network Behavior Analysis (NBA) with Sandboxing 8 187 Integration Requirements	The solution shall have support for STIX/TAXII and integration with threat intelligence platforms.	The solution shall have support for STIX/TAXII and integration with threat intelligence platforms or bidder shell quote threat Intel platform from day one. Remarks: no as it can create issue with ML	No Change.
79	3.0.1 External Attack Surface Management 9	The solution shall have feature to create template for custom report generation	The solution shall have feature to filtered report by date range, keywords, categories, and relevance to security threat for report generation	Refer to Addendum No.1 of RFP Document

Digital Government & Economy Enhancing Project
BCC
ICT Division

	220 Dashboard and Reporting			
80	Malware Analysis Sandbox (Onpremise) 7 222 Analysis Capabilities	The solution must support pre populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses.	The solution must support pre populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses. Bidder will quote the all the nenessary license to run the system with full functionality from day one.	Refer to Addendum No. 58.
81	3.7.28 Malware Analysis Sandbox (Onpremise) 7 222 Analysis Capabilities	The solution shall have feature to add custom YARA and SIGMA rules to detect emerging malware	The solution shall have feature to add custom rule like YARA or SIGMA rules to detect emerging malware Remarks: Yara is supported	YARA or SIGMA is Not Acceptable. It must be YARA and SIGMA.
82	3.7.28 Malware Analysis Sandbox (Onpremise) 8 223 File and Protocol Support	The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through inbuilt MTTM proxy.	The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through inbuilt MTTM proxy or integration of network security devices	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project ★ BCC ICT Division

83	3.7.28 Malware Analysis Sandbox (Onpremise) 9 223 Integration and Reporting	The proposed solution should have the ability to display the geolocation of identified command and control servers when possible.	The proposed solution should have the ability to display the geolocation of identified command and control servers with the help of network	Refer to Addendum No.1 of RFP Document
84	3.7.28 Malware Analysis Sandbox (Onpremise) 9 223 Integration and Reporting	The proposed solution should capture and store network traffic relevant to the analysis of detected threats, including packet captures (PCAPs).	Request to remove the line as it is a NDR features and NDR is quoting seperately. Remarks: NDR feature	Not Agreed. As most sandbox solutions inherently provide PCAP capture for threat analysis.

Enhancing Digital Government & Economy Project * BCC ICT Division

85	Malware Analysis Sandbox (Onpremise) 10 224 Compliance and Data Protection	The solution must provide compliance assurance, including clear policies for sample data retention, anonymization, and deletion upon request.	Request to remove the line as it is a OEM internal policy and customer have the full admin control of the proposed onprem solution	The request for deletion is not reasonable. The feature is asked for the solution not for supplier.
86	3.7.22 Video wall System 1 205 Pixel Pitch	min 0.5 mm	Minimum 0.63 mm (H) × 0.63 mm (V) Remarks: Market Standard for Video Wall	Refer to Addendum No.1 of RFP Document
87	3.7.22 Video wall system 1 205 Physical Seam	Min. 0.6 mm	0.88 mm (ultra-narrow bezel design) Remarks: Market Standard for Video Wall	Refer to Addendum No.1 of RFP Document
88	3.7.22 Video wall system 1 205 Resolution	at least 4K (3840x2160)	1920×1080 (FHD) Remarks: Market Standard for Video Wall	Refer to Addendum No.1 of RFP Document

89	3.7.22 Video wall system 1 206 Casing Material	SGCC	SGCC / Metal Remarks: Market Standard for Video Wall	Refer to Addendum No.1 of RFP Document
90	Page , 3.7.1 Security Information and Event Management (SIEM) (Solution Type)	On premise Self-hosted	Public Cloud Justification for Change: To effectively support the onboarding of 34 Critical Information Infrastructures (CIIs), Bangladesh's national SOC should adopt a cloud-based platform instead of on-premises technology, as it offers **scalable architecture, real-time access to global threat intelligence, and built-in AI/ML capabilities for advanced threat detection and automated response—ensuring faster deployment, lower total cost of ownership, and future-proofing against evolving cyber threats.** **Scalability for 34 CII's:** Cloud-native SOCs offer elastic scalability to onboard all 34 CII without hardware limitations or performance bottlenecks. **Built-in AI & ML Capabilities:** Cloud platforms provide advanced AI/ML for real-time threat detection, behavioral analytics, and automated incident response—capabilities that are cant be replicated to on-prem. **Access to Global Threat Intelligence:** Cloud SOCs integrate with global threat intelligence feeds, enabling faster detection of emerging threats, including zero-day and nation-state	Please refer query response number 26.

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

			attacks which onprem technology cant provide. **Faster Deployment & Lower TCO:** Cloud solutions reduce time-to-deploy from months to weeks and eliminate CapEx on infrastructure, offering a more cost-effective and agile model. **High Availability & Resilience:** Cloud platforms offer built-in redundancy, disaster recovery, and 24/7 uptime—critical for national-level cyber defense- double investment would required for site-wise redundency, disester recovery **Compliance & Security Standards:** Leading cloud SOCs are certified for global standards (ISO 27001, SOC 3, GDPR, etc.), ensuring compliance with both international and local regulations. **Future-Proof Architecture:** Cloud platforms evolve continuously with new features, integrations, and threat models, ensuring long-term adaptability and innovation.	
91	Page 147, 3.7.1 Security Information and Event Management (SIEM) (Security and Compliance)	The proposed SIEM solution shall meet the standard (PCI DSS, ISO 27001, NIST CSF etc.) and out-of-box compliance.	SOC 1, SOC 2, SOC 3 – Service Organization Controls HIPAA – U.S. healthcare data protection ISO/IEC 27001, 27017, 27018 – Information security and cloud privacy Justification for Change: SOC, PCI DSS, ISO, IEC certifications are critical in selecting products for a national SOC because they ensure compliance, security assurance, operational readiness, and vendor accountability—essential for protecting national infrastructure and citizen data. **Complying with SOC 1, SOC 2, SOC 3, HIPAA, ISO/IEC 27017, and 27018 alongside PCI DSS, ISO**	Please refer query response number 27.

			27001, and NIST CSF strengthens SIEM solution security. It broadens compliance scope to cloud readiness, healthcare privacy, and service reliability. This approach meets multiple regulatory demands, ensures data protection, robust audit trails, and trust. Business justification emphasizes risk mitigation, governance, and operational excellence. Extended standards support cloud and hybrid models, secure vendor services, advanced encryption, threat intelligence, and compliance transparency. It positions NSOC to handle diverse data types confidently, ensuring comprehensive controls, excellent service delivery, and readiness for evolving threats.	
92	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Licensing Option)	"The supplier can offer any flexible and scalable licensing model based on the following baseline information: Log Data Volume: 1500+ GB/day EPS: 40,000 or unlimited EPS Retention: 30 days before archival Redundancy factor: 1 - Unlimited log sources and EPS value "	"Log Ingestion Breakdown Timeline as Follows- A. 3 month EPS size B. 6 months EPS size C. 9 months EPS size D. 18 months EPS size E. 26 months EPS size F. 36 months EPS size Retention Analytics Log- suggest to keep 90 days" Justification for Change: The current specification of 1,500 GB/day log ingestion **from day one is unrealistic**, as log volume will gradually increase over time with the phased onboarding of all CIIs—a process expected to span several years. To ensure cost-effectiveness and operational realism, we propose a month-wise log ingestion	Refer to Addendum No. 18. .

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			model, aligned with the actual onboarding timeline. This phased approach avoids overprovisioning and ensures optimal resource utilization. Additionally, setting the analytics log retention period to 90 days strikes the right balance between: Effective threat detection and forensic investigation Trend analysis and compliance Storage efficiency and cost control This revised model ensures the National SOC remains agile, scalable, and sustainable, while meeting evolving security demands without compromising performance or budget	
93	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for SIEM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as SIEM solution from Gartner's Leader Quadrant can ensures the followings: **Proven reliability, scalability, and compliance** with global standards **Superior threat detection, analytics, and governance capabilities**—critical for national-level SOC operations **High customer satisfaction, continuous innovation, and long-term vendor support** In contrast, Visionary quadrant solutions, while innovative, **may lack the operational maturity,**	Refer to Addendum No. 1 of RFP Document.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			integration readiness, and proven scalability required for a national SOC. These solutions often carry higher implementation risks and may not meet the stringent demands of national cybersecurity infrastructure.	
94	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (Deployment Option)	On premise	Public Cloud Justification for Changes: **SOAR capabilities must be cloud-native** to ensure real-time access to AI/ML engines, which are essential for automating threat detection, response workflows, and data protection at national scale. Cloud-based SOAR platforms offer **built-in automation, adaptive playbooks, and continuous learning models**, enabling faster and more intelligent incident response. In contrast, **on-premises SOAR solutions often lack real-time AI/ML integration**, limiting their ability to adapt to evolving threats and automate complex workflows effectively. This shift ensures the NSOC remains **agile, intelligent, and future-ready,** while reducing operational complexity and enhancing national cyber resilience.	Please refer query response number 30.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

95	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (Licensing Option)	On premise license for 50 analysts from day and shall be scalable in the future	Suggesting to have unlimited licences for SOC analyst which can extended to CII's as if required Justification for Changes: **Scalable CII Onboarding:** An unlimited SOAR license allows the NSOC to assign access to CIIs as needed, without being constrained by license limits—supporting flexible, phased onboarding across all 34 CIIs. **Future-Proofing Operations:** A limited license model would restrict automation capabilities as the platform scales, potentially delaying incident response and increasing operational risk over time. **Unified Licensing for SIEM + SOAR + UEBA:** Bundling these core components under a single license model ensures: - Cost efficiency through simplified procurement and predictable budgeting - Operational agility with seamless integration and centralized management - Simplified governance and compliance tracking across the entire security stack **Strategic Value:** Unlimited licensing ensures the NSOC remains agile, scalable, and responsive to evolving national cybersecurity needs—without the administrative burden or cost spikes of license expansion.	Please refer query response number 31.

8

96	Page 149, 3.7.3 Privileged Access Management (PAM) (NA)		Identity and Access Management (IAM) is the foundational /1st layer of any Security Operations Center (SOC) including with the capabilities of Privileged Access Management (PAM). Justification for Changes: Identity and Access Management (IAM) is foundational to SOC operations, managing all user identities and access—while PAM only secures privileged accounts. PAM without IAM lacks context, making it ineffective for enforcing least privilege or detecting identity-based threats. Including IAM ensures centralized identity governance, supports Zero Trust architecture, and enables scalable, secure onboarding of CIIs. A combined IAM + PAM approach enhances visibility, compliance, and operational efficiency, making it essential for a national SOC.	Please refer query response number 32.
97	Page 149, 3.7.3 Privileged Access Management (PAM) (License)	The proposed solution should be offered for 50 admin user license with unlimited device support for 3 years	The proposed solution should be offered for 50 user IAM including PAM license for 3 years Justification for Changes:	Please refer query response number 33.
98	Page 149, 3.7.3 Privileged Access Management (PAM) (Deployment)	Bidder must provide installation and implement high availability in Active-Active mode and solution should be on-premise appliance or VM based deployment	Bidder must provide solutions in Cloud with high-availability, redundency, 99.9% uptime Justification for Changes: As outlined in section 3.7.3, the Identity and Access Management (IAM) solution, including (PAM), should be deployed as a cloud-based platform. The deployment must ensure high	Please refer query response number 34.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

			availability, redundancy, and a minimum uptime SLA of 99.9%, to meet the reliability and resilience requirements of a national-scale SOC	
99	Page 149, 3.7.3 Privileged Access Management (PAM) (General features)	Solution must be from leaders quadrant of Gartner report for PAM	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for IAM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as IAM solution from Gartner's Leader Quadrant can ensures the followings: Gartner Leaders offer **proven, end-to-end IAM capabilities with operational maturity, scalability, and integration readiness**—essential for a national SOC while Visionary vendors, often lack the depth, stability, and full feature set needed to deliver a complete, secure, and compliant IAM solution at scale. Selecting a **Leader ensures lower risk, better support, and long-term value, aligning with the NSOC's** mission for resilience, compliance, and operational excellence.	Please refer query response number 35.
100	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (NA)		The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for EDR published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as EDR solution from Gartner's Leader Quadrant can ensures the followings: **Gartner Leaders** offer **proven, scalable, and fully integrated EDR capabilities**, essential for national-level threat detection and response while	Please refer query response number 29.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			Visionary vendors often **lack the maturity, reliability, and ecosystem integration** needed for a complete and secure deployment. Choosing a **Leader ensures lower risk, better support, and long-term value,** aligning with the NSOC's mission for resilience, compliance, and operational excellence.	
101	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (General requirement)	The proposed solution should be on premises solution but will protect all type of server (physical, virtual, cloud) from a single console.	The proposed solution should be Cloud agnostic but will protect all type of users, servers, applications (physical, virtual, cloud) from a single console. Justification for Changes: We are recommending NSOC to follow the Cyber Ordinance 2025 Act 5(Cha) guidance while building national SOC. "এই অধ্যাদেশের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অন্যালিসিস এর নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুশন (যেমন - Security Information & ইভেন্ট ম্যানেজমেন্ট-SIEM, Security Orchestration, Automation, and Response-SOAR, Endpoint Detection and Response -EDR)/Extended Detection and Response -XDR, Network Detection and Response -NDR , ইত্যাদি) ব্যবহার এবং লগ আদান প্রদানের উদ্যোগ গ্রহণ "	As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.
102	3.7.10-3.7.15, 3.7.18 & 3.7.19 Server Farm Switch (Qty. 4) FC Switch (Qty. 02)		NOT REQUIRED: Cloud solutions doesnt required any of these hardware components Justification for Changes:	Please refer query response number 38.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Perimeter Switch for CII Integration (Qty. 2) Access Switch for SOC Room and Management (Qty. 2) Virtualization Software Physical Servers for on premise SOC tools (Qty. 8) FC Storage (Qty. 01) 42U Server Rack (Qty. 02)		"Recommendation to Remove On-Premise Hardware: In light of the proposed shift to cloud-based solutions, we also recommend removing the associated on-premises hardware requirements that were originally intended to support on-premises requirement. Cloud solutions will ensure required hardware capacity from the Cloud itself without incurring any additional cost to NSOC"	
103	Page 152, 3.7.28 Malware Analysis Sandbox (On-premise) (Deployment Option)	On premise	Cloud Justification for Changes: Cloud-based solutions, delivered as SaaS, eliminate the need for baseline installation and instead require only configuration to onboard servers and users from CIIs. Unlike fixed on-premise setups, cloud platforms offer elastic compute power to handle high-volume data, real-time threat intelligence updates, and seamless integration with SIEM and SOAR. This approach reduces hardware maintenance, accelerates threat analysis, enhances global accessibility and disaster recovery, and supports continuous automation, centralized management, and rapid deployment of new detection techniques—making it the most agile, efficient, and future-ready model for NSOC operations.	Please refer query response number 39.

8

104	Page 152, 3.7.31 Installation & Implementation of NSOC System (Scope of Work)	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Storage, Servers, Switches, Workstations, Video Wall, Surveillance Systems, and related infrastructure.	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Workstations, Video Wall, Surveillance Systems, and related infrastructure. Justification for Changes: "To establish a truly modern and future-ready Security Operations Center (SOC) for the government, it is essential to incorporate several additional components that are currently missing from the existing plan. We would be pleased to offer complimentary consultancy services to help identify and design the most suitable cloud-based SOC architecture. Our approach includes recommending a multi-tenant model, where each government agency operates within its own secure and isolated tenant. This structure empowers agencies with greater autonomy to manage their infrastructure while maintaining centralized oversight and collaboration with the ICT National SOC team. We are confident that this model will enhance operational efficiency, scalability, and security across all participating agencies."	Please refer query response number 40.
105	Page , 3.7.1 Security Information and Event	On premise Self-hosted	Public Cloud Justification for Change:	Please refer query response number 26.

	Management (SIEM) (Solution Type)		To effectively support the onboarding of 34 Critical Information Infrastructures (CIIs), Bangladesh's national SOC should adopt a cloud-based platform instead of on-premises technology, as it offers **scalable architecture, real-time access to global threat intelligence, and built-in AI/ML capabilities for advanced threat detection and automated response—ensuring faster deployment, lower total cost of ownership, and future-proofing against evolving cyber threats.** **Scalability for 34 CII's:** Cloud-native SOCs offer elastic scalability to onboard all 34 CII without hardware limitations or performance bottlenecks. **Built-in AI & ML Capabilities:** Cloud platforms provide advanced AI/ML for real-time threat detection, behavioral analytics, and automated incident response—capabilities that are cant be replicated to on-prem. **Access to Global Threat Intelligence:** Cloud SOCs integrate with global threat intelligence feeds, enabling faster detection of emerging threats, including zero-day and nation-state attacks which onprem technology cant provide. **Faster Deployment & Lower TCO:** Cloud solutions reduce time-to-deploy from months to weeks and eliminate CapEx on infrastructure, offering a more cost-effective and agile model. **High Availability & Resilience:** Cloud platforms offer built-in redundancy, disaster recovery, and 24/7 uptime—critical for national-level cyber defense- double investment would	

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			required for site-wise redundency, disester recovery **Compliance & Security Standards:** Leading cloud SOCs are certified for global standards (ISO 27001, SOC 3, GDPR, etc.), ensuring compliance with both international and local regulations. **Future-Proof Architecture:** Cloud platforms evolve continuously with new features, integrations, and threat models, ensuring long-term adaptability and innovation.	
106	Page 147, 3.7.1 Security Information and Event Management (SIEM) (Security and Compliance)	The proposed SIEM solution shall meet the standard (PCI DSS, ISO 27001, NIST CSF etc.) and out-of-box compliance.	SOC 1, SOC 2, SOC 3 – Service Organization Controls HIPAA – U.S. healthcare data protection ISO/IEC 27001, 27017, 27018 – Information security and cloud privacy Justification for Change: SOC, PCI DSS, ISO, IEC certifications are critical in selecting products for a national SOC because they ensure compliance, security assurance, operational readiness, and vendor accountability—essential for protecting national infrastructure and citizen data. **Complying with SOC 1, SOC 2, SOC 3, HIPAA, ISO/IEC 27017, and 27018 alongside PCI DSS, ISO 27001, and NIST CSF strengthens SIEM solution security**. It broadens compliance scope to cloud readiness, healthcare privacy, and service reliability. This approach meets multiple regulatory demands, ensures data protection, robust audit trails, and trust. Business justification emphasizes risk mitigation, governance, and operational excellence. Extended standards support cloud and hybrid models, secure vendor	Please refer query response number 27. And Refer to Addendum No. 16.

			services, advanced encryption, threat intelligence, and compliance transparency. It positions NSOC to handle diverse data types confidently, ensuring comprehensive controls, excellent service delivery, and readiness for evolving threats.	
107	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Licensing Option)	"The supplier can offer any flexible and scalable licensing model based on the following baseline information: Log Data Volume: 1500+ GB/day EPS: 40,000 or unlimited EPS Retention: 30 days before archival Redundancy factor: 1 - Unlimited log sources and EPS value "	"Log Ingestion Breakdown Timeline as Follows- A. 3 month EPS size B. 6 months EPS size C. 9 months EPS size D. 18 months EPS size E. 26 months EPS size F. 36 months EPS size Retention Analytics Log- suggest to keep 90 days" Justification for Change: The current specification of 1,500 GB/day log ingestion **from day one is unrealistic**, as log volume will gradually increase over time with the phased onboarding of all CIIs—a process expected to span several years. To ensure cost-effectiveness and operational realism, we propose a month-wise log ingestion model, aligned with the actual onboarding timeline. This phased approach avoids overprovisioning and ensures optimal resource utilization. Additionally, setting the analytics log retention period to 90 days strikes the right balance between: Effective threat detection and forensic	Refer to Addendum No. 18 .

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			investigation Trend analysis and compliance Storage efficiency and cost control This revised model ensures the National SOC remains agile, scalable, and sustainable, while meeting evolving security demands without compromising performance or budget	
108	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for SIEM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as SIEM solution from Gartner's Leader Quadrant can ensures the followings: **Proven reliability, scalability, and compliance** with global standards **Superior threat detection, analytics, and governance capabilities**—critical for national-level SOC operations **High customer satisfaction, continuous innovation, and long-term vendor support** In contrast, Visionary quadrant solutions, while innovative, **<u>may lack the operational maturity, integration readiness, and proven scalability</u>** required for a national SOC. These solutions often carry higher implementation risks and may not meet the stringent demands of national cybersecurity infrastructure.	Refer to Addendum No. 19
109	Page 154, 3.7.2 Security Orchestration,	On premise	Public Cloud Justification for Changes:	Please refer query response number 30.

Enhancing Digital Government & Economy Project
BCC
ICT Division

8

	Automation, and Response (SOAR) (Deployment Option)		**SOAR capabilities must be cloud-native** to ensure real-time access to AI/ML engines, which are essential for automating threat detection, response workflows, and data protection at national scale. Cloud-based SOAR platforms offer **built-in automation, adaptive playbooks, and continuous learning models**, enabling faster and more intelligent incident response. In contrast, **on-premises SOAR solutions often lack real-time AI/ML integration**, limiting their ability to adapt to evolving threats and automate complex workflows effectively. This shift ensures the NSOC remains **agile, intelligent, and future-ready,** while reducing operational complexity and enhancing national cyber resilience.	

110	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (Licensing Option)	On premise license for 50 analysts from day and shall be scalable in the future	Suggesting to have unlimited licences for SOC analyst which can extended to CII's as if required Justification for Changes: **Scalable CII Onboarding:** An unlimited SOAR license allows the NSOC to assign access to CIIs as needed, without being constrained by license limits—supporting flexible, phased onboarding across all 34 CIIs. **Future-Proofing Operations:** A limited license model would restrict automation capabilities as the platform scales, potentially delaying incident response and increasing operational risk over time. **Unified Licensing for SIEM + SOAR + UEBA:** Bundling these core components under a single license model ensures: - Cost efficiency through simplified procurement and predictable budgeting - Operational agility with seamless integration and centralized management - Simplified governance and compliance tracking across the entire security stack **Strategic Value:** Unlimited licensing ensures the NSOC remains agile, scalable, and responsive to evolving national cybersecurity needs—without the administrative burden or cost spikes of license expansion.	Please refer query response number 31.

Enhancing Digital Government & Economy Project * BCC ICT Division

111	Page 149, 3.7.3 Privileged Access Management (PAM) (NA)		Identity and Access Management (IAM) is the foundational /1st layer of any Security Operations Center (SOC) including with the capabilities of Privileged Access Management (PAM). Justification for Changes: Identity and Access Management **(IAM) is foundational** to SOC operations, managing all user identities and access—while PAM only secures privileged accounts. **PAM without IAM lacks context**, making it ineffective for enforcing least privilege or detecting identity-based threats. Including **IAM ensures centralized identity governance, supports Zero Trust architecture,** and enables scalable, secure onboarding of CIIs. A **combined IAM + PAM approach enhances visibility, compliance, and operational efficiency,** making it essential for a national SOC.	Please refer query response number 32.
112	Page 149, 3.7.3 Privileged Access Management (PAM) (License)	The proposed solution should be offered for 50 admin user license with unlimited device support for 3 years	The proposed solution should be offered for 50 user IAM including PAM license for 3 years Justification for Changes:	Please refer query response number 33.
113	Page 149, 3.7.3 Privileged Access Management (PAM) (Deployment)	Bidder must provide installation and implement high availability in Active-Active mode and solution should be on-premise appliance or VM based deployment	Bidder must provide solutions in Cloud with high-availability, redundency, 99.9% uptime Justification for Changes: As outlined in section 3.7.3, the Identity and Access Management (IAM) solution, including (PAM), should be deployed as a cloud-based platform. The deployment must ensure high	Please refer query response number 34.

Enhancing Digital Government & Economy Project
BCC
ICT Division

8

			availability, redundancy, and a minimum uptime SLA of 99.9%, to meet the reliability and resilience requirements of a national-scale SOC	
114	Page 149, 3.7.3 Privileged Access Management (PAM) (General features)	Solution must be from leaders quadrant of Gartner report for PAM	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for IAM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as IAM solution from Gartner's Leader Quadrant can ensures the followings: Gartner Leaders offer **proven, end-to-end IAM capabilities with operational maturity, scalability, and integration readiness**—essential for a national SOC while Visionary vendors, often lack the depth, stability, and full feature set needed to deliver a complete, secure, and compliant IAM solution at scale. Selecting a **Leader ensures lower risk, better support, and long-term value, aligning with the NSOC's** mission for resilience, compliance, and operational excellence.	Please refer query response number 35.
115	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (NA)		The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for EDR published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as EDR solution from Gartner's Leader Quadrant can ensures the followings: **Gartner Leaders** offer **proven, scalable, and fully integrated EDR capabilities**, essential for national-level threat detection and response while	Please refer query response number 29.

			Visionary vendors often **lack the maturity, reliability, and ecosystem integration** needed for a complete and secure deployment. Choosing a **Leader ensures lower risk, better support, and long-term value,** aligning with the NSOC's mission for resilience, compliance, and operational excellence.	
116	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (General requirement)	The proposed solution should be on premises solution but will protect all type of server (physical, virtual, cloud) from a single console.	The proposed solution should be Cloud agnostic but will protect all type of users, servers, applications (physical, virtual, cloud) from a single console. Justification for Changes: We are recommending NSOC to follow the Cyber Ordinance 2025 Act 5(Cha) guidance while building national SOC. "এই অধ্যাদেশের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অন্যালিসিস এর নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুশন (যেমন - Security Information & ইভেন্ট ম্যানেজমেন্ট-SIEM, Security Orchestration, Automation, and Response-SOAR, Endpoint Detection and Response -EDR)/Extended Detection and Response -XDR, Network Detection and Response -NDR , ইত্যাদি) ব্যবহার এবং লগ আদান প্রদানের উদ্যোগ গ্রহণ "	Please refer query response number 37.

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

117	3.7.10-3.7.15, 3.7.18 & 3.7.19 Server Farm Switch (Qty. 4) FC Switch (Qty. 02) Perimeter Switch for CII Integration (Qty. 2) Access Switch for SOC Room and Management (Qty. 2) Virtualization Software Physical Servers for on premise SOC tools (Qty. 8) FC Storage (Qty. 01) 42U Server Rack (Qty. 02)		NOT REQUIRED: Cloud solutions doesnt required any of these hardware components Justification for Changes: "Recommendation to Remove On-Premise Hardware: In light of the proposed shift to cloud-based solutions, we also recommend removing the associated on-premises hardware requirements that were originally intended to support on-premises requirement. Cloud solutions will ensure required hardware capacity from the Cloud itself without incurring any additional cost to NSOC"	Please refer query response number 38.
118	Page 152, 3.7.28 Malware Analysis Sandbox (On-premise) (Deployment Option)	On premise	Public Cloud Justification for Changes: Cloud-based solutions, delivered as SaaS, eliminate the need for baseline installation and instead require only configuration to onboard servers and users from CIIs. Unlike fixed on-premise setups, cloud platforms offer elastic compute power to handle high-volume data, real-	Please refer query response number 39.

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

			time threat intelligence updates, and seamless integration with SIEM and SOAR. This approach reduces hardware maintenance, accelerates threat analysis, enhances global accessibility and disaster recovery, and supports continuous automation, centralized management, and rapid deployment of new detection techniques—making it the most agile, efficient, and future-ready model for NSOC operations.	

119	Page 152, 3.7.31 Installation & Implementation of NSOC System (Scope of Work)	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Storage, Servers, Switches, Workstations, Video Wall, Surveillance Systems, and related infrastructure.	Complete installation, configuration, testing, and commissioning of all NSOC components including: SIEM, SOAR, UEBA, PAM, EDR, NBA, Firewalls, Workstations, Video Wall, Surveillance Systems, and related infrastructure. Justification for Changes: "To establish a truly modern and future-ready Security Operations Center (SOC) for the government, it is essential to incorporate several additional components that are currently missing from the existing plan. We would be pleased to offer complimentary consultancy services to help identify and design the most suitable cloud-based SOC architecture. Our approach includes recommending a multi-tenant model, where each government agency operates within its own secure and isolated tenant. This structure empowers agencies with greater autonomy to manage their infrastructure while maintaining centralized oversight and collaboration with the ICT National SOC team. We are confident that this model will enhance operational efficiency, scalability, and security across all participating agencies."	Please refer query response number 40.

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
120	Page , 3.7.1 Security Information and Event Management (SIEM) (Solution Type)	On premise Self-hosted	Public Cloud Justification for Change: To effectively support the onboarding of 34 Critical Information Infrastructures (CIIs), Bangladesh's national SOC should adopt a cloud-based platform instead of on-premises technology, as it offers **scalable architecture, real-time access to global threat intelligence, and built-in AI/ML capabilities for advanced threat detection and automated response—ensuring faster deployment, lower total cost of ownership, and future-proofing against evolving cyber threats.** **Scalability for 34 CII's:** Cloud-native SOCs offer elastic scalability to onboard all 34 CII without hardware limitations or performance bottlenecks. **Built-in AI & ML Capabilities:** Cloud platforms provide advanced AI/ML for real-time threat detection, behavioral analytics, and automated incident response—capabilities that are cant be replicated to on-prem. **Access to Global Threat Intelligence:** Cloud SOCs integrate with global threat intelligence feeds, enabling faster detection of emerging threats, including zero-day and nation-state attacks which onprem technology cant provide. **Faster Deployment & Lower TCO:** Cloud solutions reduce time-to-deploy from months to weeks and eliminate CapEx on infrastructure, offering a more cost-effective and agile model.	Please refer query response number 26

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			High Availability & Resilience: Cloud platforms offer built-in redundancy, disaster recovery, and 24/7 uptime—critical for national-level cyber defense-double investment would required for site-wise redundency, disester recovery **Compliance & Security Standards:** Leading cloud SOCs are certified for global standards (ISO 27001, SOC 3, GDPR, etc.), ensuring compliance with both international and local regulations. **Future-Proof Architecture:** Cloud platforms evolve continuously with new features, integrations, and threat models, ensuring long-term adaptability and innovation.	

Enhancing Digital Government & Economy
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
121	Page 147, 3.7.1 Security Information and Event Management (SIEM) (Security and Compliance)	The proposed SIEM solution shall meet the standard (PCI DSS, ISO 27001, NIST CSF etc.) and out-of-box compliance.	SOC 1, SOC 2, SOC 3 – Service Organization Controls HIPAA – U.S. healthcare data protection ISO/IEC 27001, 27017, 27018 – Information security and cloud privacy Justification for Change: SOC, PCI DSS, ISO, IEC certifications are critical in selecting products for a national SOC because they ensure compliance, security assurance, operational readiness, and vendor accountability—essential for protecting national infrastructure and citizen data. **Complying with SOC 1, SOC 2, SOC 3, HIPAA, ISO/IEC 27017, and 27018 alongside PCI DSS, ISO 27001, and NIST CSF strengthens SIEM solution security**. It broadens compliance scope to cloud readiness, healthcare privacy, and service reliability. This approach meets multiple regulatory demands, ensures data protection, robust audit trails, and trust. Business justification emphasizes risk mitigation, governance, and operational excellence. Extended standards support cloud and hybrid models, secure vendor services, advanced encryption, threat intelligence, and compliance transparency. It positions NSOC to handle diverse data types confidently, ensuring comprehensive controls, excellent service delivery, and readiness for evolving threats.	Please refer query response number 27

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
122	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Licensing Option)	"The supplier can offer any flexible and scalable licensing model based on the following baseline information: Log Data Volume: 1500+ GB/day EPS: 40,000 or unlimited EPS Retention: 30 days before archival Redundancy factor: 1 - Unlimited log sources and EPS value "	"Log Ingestion Breakdown Timeline as Follows- A. 3 month EPS size B. 6 months EPS size C. 9 months EPS size D. 18 months EPS size E. 26 months EPS size F. 36 months EPS size Retention Analytics Log- suggest to keep 90 days" Justification for Change: The current specification of 1,500 GB/day log ingestion **from day one is unrealistic**, as log volume will gradually increase over time with the phased onboarding of all CIIs—a process expected to span several years. To ensure cost-effectiveness and operational realism, we propose a month-wise log ingestion model, aligned with the actual onboarding timeline. This phased approach avoids overprovisioning and ensures optimal resource utilization. Additionally, setting the analytics log retention period to 90 days strikes the right balance between: Effective threat detection and forensic investigation Trend analysis and compliance Storage efficiency and cost control This revised model ensures the National SOC remains agile, scalable, and sustainable, while	Refer to Addendum No. 18 .

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			meeting evolving security demands without compromising performance or budget	
123	Page 148, 3.7.1 Security Information and Event Management (SIEM) (Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for SIEM published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as SIEM solution from Gartner's Leader Quadrant can ensures the followings: **Proven reliability, scalability, and compliance** with global standards **Superior threat detection, analytics, and governance capabilities**—critical for national-level SOC operations **High customer satisfaction, continuous innovation, and long-term vendor support** In contrast, Visionary quadrant solutions, while innovative, **may lack the operational maturity, integration readiness, and proven scalability** required for a national SOC. These solutions often carry higher implementation risks and may not meet the stringent demands of national cybersecurity infrastructure.	Refer to Addendum No. 19.
124	Page 154, 3.7.2 Security Orchestration, Automation, and Response	On premise	Public Cloud Justification for Changes:	Please refer query response number 30

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	(SOAR) (Deployment Option)		**SOAR capabilities must be cloud-native** to ensure real-time access to AI/ML engines, which are essential for automating threat detection, response workflows, and data protection at national scale. Cloud-based SOAR platforms offer **built-in automation, adaptive playbooks, and continuous learning models**, enabling faster and more intelligent incident response. In contrast, **on-premises SOAR solutions often lack real-time AI/ML integration**, limiting their ability to adapt to evolving threats and automate complex workflows effectively. This shift ensures the NSOC remains **agile, intelligent, and future-ready,** while reducing operational complexity and enhancing national cyber resilience.	
125	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (Licensing Option)	On premise license for 50 analysts from day and shall be scalable in the future	Suggesting to have unlimited licences for SOC analyst which can extended to CII's as if required Justification for Changes: **Scalable CII Onboarding:** An unlimited SOAR license allows the NSOC to assign access to CIIs as needed, without being constrained by license limits—supporting flexible, phased onboarding across all 34 CIIs. **Future-Proofing Operations:** A limited license model would restrict automation capabilities as the platform scales, potentially delaying incident	Please refer query response number 31

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			response and increasing operational risk over time. **Unified Licensing for SIEM + SOAR + UEBA:** Bundling these core components under a single license model ensures: - Cost efficiency through simplified procurement and predictable budgeting - Operational agility with seamless integration and centralized management - Simplified governance and compliance tracking across the entire security stack **Strategic Value:** Unlimited licensing ensures the NSOC remains agile, scalable, and responsive to evolving national cybersecurity needs—without the administrative burden or cost spikes of license expansion.	
126	Page 149, 3.7.3 Privileged Access Management (PAM) (NA)		Identity and Access Management (IAM) is the foundational /1st layer of any Security Operations Center (SOC) including with the capabilities of Privileged Access Management (PAM). Justification for Changes: Identity and Access Management **(IAM) is foundational** to SOC operations, managing all user identities and access—while PAM only secures privileged accounts. **PAM without IAM lacks context**, making it ineffective for enforcing least privilege or detecting identity-based threats.	Please refer query response number 32

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Including **IAM ensures centralized identity governance, supports Zero Trust architecture,** and enables scalable, secure onboarding of CIIs. A **combined IAM + PAM approach enhances visibility, compliance, and operational efficiency,** making it essential for a national SOC.	
127	Page 149, 3.7.3 Privileged Access Management (PAM) (License)	The proposed solution should be offered for 50 admin user license with unlimited device support for 3 years	The proposed solution should be offered for 50 user IAM including PAM license for 3 years Justification for Changes:	Please refer query response number 33
128	Page 149, 3.7.3 Privileged Access Management (PAM) (Deployment)	Bidder must provide installation and implement high availability in Active-Active mode and solution should be on-premise appliance or VM based deployment	Bidder must provide solutions in Cloud with high-availability, redundency, 99.9% uptime Justification for Changes: As outlined in section 3.7.3, the Identity and Access Management (IAM) solution, including (PAM), should be deployed as a cloud-based platform. The deployment must ensure high availability, redundancy, and a minimum uptime SLA of 99.9%, to meet the reliability and resilience requirements of a national-scale SOC	Please refer query response number 34
129	Page 149, 3.7.3 Privileged Access Management (PAM) (General features)	Solution must be from leaders quadrant of Gartner report for PAM	The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for IAM published in 2024 Justification for Changes:	Please refer to query response number 35.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			We recommend limiting it with Gartner Leaders only as IAM solution from Gartner's Leader Quadrant can ensures the followings: Gartner Leaders offer **proven, end-to-end IAM capabilities with operational maturity, scalability, and integration readiness**—essential for a national SOC while Visionary vendors, often lack the depth, stability, and full feature set needed to deliver a complete, secure, and compliant IAM solution at scale. Selecting a **Leader ensures lower risk, better support, and long-term value, aligning with the NSOC's** mission for resilience, compliance, and operational excellence.	
130	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (NA)		The offered solution shall be positioned in the leader quadrant of latest Gartner Magic Quadrants for EDR published in 2024 Justification for Changes: We recommend limiting it with Gartner Leaders only as EDR solution from Gartner's Leader Quadrant can ensures the followings: **Gartner Leaders** offer **proven, scalable, and fully integrated EDR capabilities**, essential for national-level threat detection and response while Visionary vendors often **lack the maturity, reliability, and ecosystem integration** needed for a complete and secure deployment. Choosing a **Leader ensures lower risk, better support, and long-term value,** aligning with the	Please refer query response number 29

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			NSOC's mission for resilience, compliance, and operational excellence.	
131	Page 150, 3.7.4 Endpoint Detection and Response (EDR) (General requirement)	The proposed solution should be on premises solution but will protect all type of server (physical, virtual, cloud) from a single console.	The proposed solution should be Cloud agnostic but will protect all type of users, servers, applications (physical, virtual, cloud) from a single console. Justification for Changes: We are recommending NSOC to follow the Cyber Ordinance 2025 Act 5(Cha) guidance while building national SOC. "এই অধ্যাদেশের উদ্দেশ্য পূরণকল্পে, কাউন্সিলের অনুমোদন গ্রহণক্রমে, সিকিউরিটি অন্যালিসিস এর নিমিত্তে ক্লাউডভিত্তিক সাইবার সিকিউরিটি সল্যুশন (যেমন - Security Information & ইভেন্ট ম্যানেজমেন্ট-SIEM, Security Orchestration, Automation, and Response-SOAR, Endpoint Detection and Response -EDR)/Extended Detection and Response -XDR, Network Detection and Response -NDR , ইত্যাদি) ব্যবহার এবং লগ আদান প্রদানের উদ্যোগ গ্রহণ "	Please refer query response number 37 As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border.
132	3.7.10-3.7.15, 3.7.18 & 3.7.19 Server Farm Switch (Qty. 4) FC Switch (Qty. 02) Perimeter Switch for CII Integration (Qty. 2)		NOT REQUIRED: Cloud solutions doesnt required any of these hardware components Justification for Changes: "Recommendation to Remove On-Premise Hardware: In light of the proposed shift to cloud-based solutions, we also recommend removing the associated on-	Please refer query response number 38

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Access Switch for SOC Room and Management (Qty. 2) Virtualization Software Physical Servers for on premise SOC tools (Qty. 8) FC Storage (Qty. 01) 42U Server Rack (Qty. 02)		premises hardware requirements that were originally intended to support on-premises requirement. Cloud solutions will ensure required hardware capacity from the Cloud itself without incurring any additional cost to NSOC"	

Enhancing Digital Government & E
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
133	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution shall support high availability, redundancy, and scalability.	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software and the solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on. Remarks: To make it more use case driven and useful to BCC NSOC. As SIEM consists of multiple modules, writing on high availability, redundancy and scalability supports are	Refer to Addendum No. 6.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
134	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution must be software-based allowing flexible deployment models and architecture.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters. Remarks: To ensure reliability and reduce TCO. As SIEM consists of multiple modules, mentioning the detail deployment model is more suitable and it will be easier to understand the proposed solution	Refer to Addendum No.1 of RFP Document
135	Page 148, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The solution shall support multi-tenancy from day 1 for separation of log ingestion, analysis, dashboard and reporting.	Please remove Remarks: Please help us understand that why in your environment a multi tenent solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Not Agreed. Since every individual CIIs will be considered as an individual tenant
136	Page 148, 3.7.1 Security Information and Event Management (SIEM)	The solution shall support parsing single-line and multi-line log files.	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	(5. Log Collection or Ingestion Capabilities)		data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce TCO and make the solution reliable and always useful. Data parsers dependencies should be imposed to OEM for better efficiency	
137	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing, normalization or filtering of data before ingestion into the system.	The proposed solution must comes with apps and ad-ons for most common /well known security technologies and OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce the TCO and ensure availability of the parsers for any kind of data. Data parsers dependencies should be imposed to OEM for better efficiency	Refer to Addendum No.1 of RFP Document
138	Page 149, 3.7.1 Security Information and Event Management (SIEM)	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization.	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	(5. Log Collection or Ingestion Capabilities)		Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time. Remarks: To make it more use case driven and useful to BCC NSOC, please change this clause as the change request	
139	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks The solution shall support multiple correlation methods like Vulnerability, Signature, Statistical, Historical, Heuristic and Predictive correlation. The solution shall have pre-built correlation rules for rapid deployment and coverage of common attack scenarios.	The proposed solution must come with at least 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems and it should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.) The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques. Remarks: Request to change this as proposed. To ensure it covers all the attck scenarios and reliable and updated to most lastest known and unknown attacks.	Refer to Addendum No.1 of RFP Document
140	Page 149, 3.7.1 Security Information	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution should be able to assign risk score with Scoring for various identified entities like user &	Refer to Addendum No.1 of RFP Document

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	and Event Management (SIEM) (6. Correlation & Detection Capabilities)		assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user. Remarks: Request to change this as proposed. To ensure the solution is robust and reduce the overall false positives greatly scientifically.	
141	Page 150, 3.7.1 Security Information and Event Management (SIEM) (7. AI/ML and UEBA Capabilities)	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats. The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time. Investigate and respond to detected threats using a streamlined threat review	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations. Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user. The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior. The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat. Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields. The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors. The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI. The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into	

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			the correct sections of the chain. The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing. The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity. The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat. UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time. Note: Bidder must comply with all the mandatory points in the technical and functional requirement as mentioned above, Non-compliance with any of the mandatory requirements may make the bid liable for rejection. Also, please understand that any of the above technical requirements mentioned needs to be demonstrated as asked during the evaluation phase. Remarks: To ensure a right solution that is useful to BCC NSOC is available and not just for the namesake, please add the technical use case driven specifications of UBA.	

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
142	Page 150, 3.7.1 Security Information and Event Management (SIEM) (8. Integration Feature)	The solution shall support integration with any SOAR platform.	The solution shall support integration with any third party solution with in-built plug ins and apps and platform and must have SOAR solution from same OEM to reduce any complexity. Remarks: Request to change this as proposed. To ensure a end to end and seamless integration please rephrase	Refer to Addendum No.1 of RFP Document
143	Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall provide pre-built SOC dashboards and have compliance-ready reports (PCI DSS, ISO 27001, NIST, GDPR).	The solution shall provide pre-built SOC dashboards like Security Posture, Incident Review and Executive Summary dashboard to help ivestigate fatser and Top officials have the SOC visibility. - The solution shall have compliance-ready reports, solution which can be configured modified as per need by the auditter by bidder. Remarks: Request to change this as proposed. To make it effective and use case driven please rephrase	Please refer to the RFP "Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)" it has provided detailed specific requirements for the Dashboard, Search & Reporting Capabilities.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
144	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall support configuring separate dashboard for each tenant.	Please remove it Remarks: Please help us understand that why in your environment a multi tenant solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Not Agreed. Since every individual CIIs will be considered as an individual tenant.
145	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements.	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: Request to change this as proposed. To make sure it follows the standard process and less dependency and more coverage.	
146	Page 152, 3.7.1 Security Information and Event Management (SIEM) (12. Licensing Option)	The supplier can offer any flexible and scalable licensing model based on the following baseline information: - Log Data Volume: 1500+ GB/day - EPS: 40,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value	Log Data Volume: 300+ GB/day - EPS: 8,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value Remarks: Requesting to please consider this proposed sizing. As all the CII will not be onboarded to the NSOC SIEM on day 1. So 1500 GB/day or 40,000 EPS are very high volume of data ingestion and will insure HUGE COST. As per our understanding, 300GB/day or 8,000 EPS should be sufficient for the operation. Kindly share the details of data sources for the right sizing of the solution for Day 1.	Please refer query response number 22

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
147	Page 152, 3.7.1 Security Information and Event Management (SIEM) (13. Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.	The offered solution shall be positioned either in the leader or Challengers quadrants for the last 5 consequtive years reports at Gartner Magic Quadrants for SIEM Remarks: Global Leaders for SIEM Solutions are listed in either Leaders or Challengers in the Gartner Magic Quadrant Reports. By adding Visionary will allow Startup solutions whose doesn't have much market references globally.	Refer to Addendum No. 1 of RFP Document.
148	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (9. Integration)	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM Remarks: Request to change this as proposed. To ensure a end to end and seamless integration same OEM is cost effective	Not Agreed.

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
149	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (10. Licensing Option)	On-premise license for 50 analysts from day one and shall be scalable in the future.	0n premise license for 5 analysts from day one and shall be scalable in the future Remarks: Request to change this as proposed. 50 analysts licenses is too high for the NSOC requirement and insure HUGE COST. 5 analysts License should be enough considering 3 shifts operation as Licenses are concurrent in nature.	Please refer query response number 31
150	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE)	The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE). Remarks: Request to change this as proposed. Windows 7 and 8, Server 2012,2016,2019(regular) support has already been discontinued by Microsoft. So requesting to remove the end of life OS	Refer to Addendum No. 26.
151	Page N/A, 3.7.9 Network Behavior Analysis (NBA) with Sandboxing	**(Not specified)**	Proposed Solution should support data retention for minimum 30 Days Remarks: Log retention or data retention period is not mentioned. Requesting to include minimum 30 days of data retention	Refer to Addendum No. 46.
152	Page 147, 3.7.1 Security Information and Event Management	The proposed solution shall support high availability, redundancy, and scalability.	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software and the solution should be	Refer to Addendum No. 6

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	(SIEM) (4. General Requirement)		DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on. Remarks: To make it more use case driven and useful to BCC NSOC. As SIEM consists of multiple modules, writing on high availability, redundancy and scalability supports are	
153	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution must be software-based allowing flexible deployment models and architecture.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters. Remarks: To ensure reliability and reduce TCO. As SIEM consists of multiple modules, mentioning the detail deployment model is more suitable and it will be easier to understand the proposed solution	Please refer query response number 134

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
154	Page 148, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The solution shall support multi-tenancy from day 1 for separation of log ingestion, analysis, dashboard and reporting.	Please remove Remarks: Please help us understand that why in your environment a multi tenent solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 135
155	Page 148, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution shall support parsing single-line and multi-line log files.	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce TCO and make the solution reliable and always useful. Data parsers dependencies should be imposed to OEM for better efficiency	Please refer query response number 136
156	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing, normalization or filtering of data before ingestion into the system.	The proposed solution must comes with apps and ad-ons for most common /well known security technologies and OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business	Please refer query response number 137

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce the TCO and ensure availability of the parsers for any kind of data. Data parsers dependencies should be imposed to OEM for better efficiency	
157	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time. Remarks: To make it more use case driven and useful to BCC NSOC, please change this clause as the change request	Please refer query response number 138
158	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks The solution shall support multiple correlation methods like Vulnerability, Signature, Statistical, Historical, Heuristic and Predictive correlation. The solution shall have pre-built correlation rules for rapid deployment and coverage of common attack scenarios.	The proposed solution must come with at least 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems and it should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.) The proposed solution should have Out of The Box	Please refer query response number 139

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques. Remarks: Request to change this as proposed. To ensure it covers all the attck scenarios and reliable and updated to most lastest known and unknown attacks.	
159	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user. Remarks: Request to change this as proposed. To ensure the solution is robust and reduce the overall false positives greatly scientifically.	Please refer query response number 140

Digital Government & Economy Enhancing Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
160	Page 150, 3.7.1 Security Information and Event Management (SIEM) (7. AI/ML and UEBA Capabilities)	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats. The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time. Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations. Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user. The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior. The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not	Please refer query response number 141

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat. Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields. The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors. The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI. The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain. The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing. The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity. The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat. UEBA should perform identity resolution to find the real-time	

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time. Note: Bidder must comply with all the mandatory points in the technical and functional requirement as mentioned above, Non-compliance with any of the mandatory requirements may make the bid liable for rejection. Also, please understand that any of the above technical requirements mentioned needs to be demonstrated as asked during the evaluation phase. Remarks: To ensure a right solution that is useful to BCC NSOC is available and not just for the namesake, please add the technical use case driven specifications of UBA.	

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
161	Page 150, 3.7.1 Security Information and Event Management (SIEM) (8. Integration Feature)	The solution shall support integration with any SOAR platform.	The solution shall support integration with any third party solution with in-built plug ins and apps and platform and must have SOAR solution from same OEM to reduce any complexity. Remarks: Request to change this as proposed. To ensure a end to end and seamless integration please rephrase	Please refer query response number 142
162	Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall provide pre-built SOC dashboards and have compliance-ready reports (PCI DSS, ISO 27001, NIST, GDPR).	The solution shall provide pre-built SOC dashboards like Security Posture, Incident Review and Executive Summary dashboard to help ivestigate fatser and Top officials have the SOC visibility. - The solution shall have compliance-ready reports, solution which can be configured modified as per need by the auditter by bidder. Remarks: Request to change this as proposed. To make it effective and use case driven please rephrase	Please refer query response number 143

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
163	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall support configuring separate dashboard for each tenant.	Please remove it Remarks: Please help us understand that why in your environment a multi tenant solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 144
164	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements.	Please refer query response number 145

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: Request to change this as proposed. To make sure it follows the standard process and less dependency and more coverage.	
165	Page 152, 3.7.1 Security Information and Event Management (SIEM) (12. Licensing Option)	The supplier can offer any flexible and scalable licensing model based on the following baseline information: - Log Data Volume: 1500+ GB/day - EPS: 40,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value	Log Data Volume: 300+ GB/day - EPS: 8,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value Remarks: Requesting to please consider this proposed sizing. As all the CII will not be onboarded to the NSOC SIEM on day 1. So 1500 GB/day or 40,000 EPS are very high volume of data ingestion and will insure HUGE COST. As per our understanding, 300GB/day or 8,000 EPS should be sufficient for the operation. Kindly share the details of data sources for the right sizing of the solution for Day 1.	Please refer query response number 22
166	Page 152, 3.7.1 Security Information and Event Management (SIEM) (13. Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.	The offered solution shall be positioned either in the leader or Challengers quadrants for the last 5 consequtive years reports at Gartner Magic Quadrants for SIEM Remarks: Global Leaders for SIEM Solutions are listed in either Leaders or Challengers in the Gartner Magic Quadrant Reports. By adding Visionary will allow Startup solutions whose doesn't have much market references globally.	Please refer query response number 29

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
167	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (9. Integration)	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM Remarks: Request to change this as proposed. To ensure a end to end and seamless integration same OEM is cost effective	Please refer query response number 148
168	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (10. Licensing Option)	On-premise license for 50 analysts from day one and shall be scalable in the future.	0n premise license for 5 analysts from day one and shall be scalable in the future Remarks: Request to change this as proposed. 50 analysts licenses is too high for the NSOC requirement and insure HUGE COST. 5 analysts License should be enough considering 3 shifts operation as Licenses are concurrent in nature.	Refer to Addendum No. 21
169	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE)	The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE). Remarks: Request to change this as proposed. Windows 7 and 8, Server 2012,2016,2019(regular)	Refer to Addendum No. 26.

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			support has already been discontinued by Microsoft. So requesting to remove the end of life OS	
170	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	EDR is a security solution which is designed to monitor, detect, and respond to threats on endpoints such as workstations, servers, and mobile devices. It provides real-time monitoring of activities like file system changes, process executions, memory operations, and network connections. The EDR uses various detection techniques including behavioral analysis, machine learning, and signature based methods to identify malicious activities. It offers automated response actions, such as process termination or file quarantine, and supports integration with SIEMs, threat intelligence platforms, and vulnerability management systems.	EDR is a security solution which is designed to monitor, detect, and respond to threats on endpoints such as workstations, servers, and mobile devices. It provides real-time monitoring of activities like file system changes, process executions, memory operations, and network connections. The EDR uses various detection techniques including behavioral analysis, machine learning, and signatureless / signature-based methods to identify malicious activities. It offers automated response actions, such as process termination or file quarantine, and supports integration withSIEMs, threat intelligence platforms, and vulnerability management systems. Remarks: Requesting the department to choose new age technology to strengthen the security posture. We suggest you includes signatureless method that should be based on AI/ML technology.	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
171	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The solution must employ multiple detection techniques including signature-based, behavioral analysis, machine learning, and IOC matching.	The solution must employ multiple detection techniques including signatureless/ signaturebased, behavioral analysis, machine learning, and IOC matching. Remarks: Requesting the department to choose new age technology to strengthen the security posture. We suggest you include signatureless methods that should be based on AI/ML technology.	Refer to Addendum No. 65.
172	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR should provide tools for credential reset or revocation when compromise is detected.	The solution should provide tools for credential reset or revocation when compromise is detected. Remarks: This is not EDR functionality. However, this can be achieved with the Identity Protection feature of SentinelOne.	Refer to Addendum No. 66.
173	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The solution should establish user behavior baselines for anomaly detection.	The solution should establish user behavior for malware detection. Remarks: We request the department to modify the clause for larger vendor participation.	Refer to Addendum No.1 of RFP Document
174	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR must detect suspicious user activities that may indicate account compromise.	The EDR must detect suspicious user/malware activities that may indicate account compromise. Remarks: We request the department to modify the clause for larger vendor participation.	Refer to Addendum No.1 of RFP Document

8

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
175	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The solution should correlate user activities across multiple endpoints to identify patterns.	The solution should correlate user/ malicious activities across multiple endpoints to identify patterns. Remarks: We request the department to modify the clause for larger vendor participation.	Refer to Addendum No. 67.
176	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The solution must include tools for load balancing and distribution.	Remarks: We request the department remove this clause as EDR is managed by the agent installed on the surface and the management console is a control plane, no requirement of traffic distribution. We suggest you go for the SaaS platform.	Not Agreed As per draft Personal Data Protection Ordinance (PDPO), 2025 , any government confidential data can not be cross border. So, Saas Based platform not consider.
177	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR should support horizontal scaling of server components.	Remarks: We request the department remove this clause as EDR is managed by the agent installed on the surface and the management console is a control plane. There is no requirement to scale the server. We suggest you go for SaaS based platform.	Not Agreed

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
178	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	and Scalability	Remarks: We request department to remove this clause as storage is managed by the vendor in case of SaaS platform. We suggest you to go for Saas-based platform.	Not Agreed
179	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The proposed solution should be offered for 1000 (One thousand) endpoints and shall be an on premise EDR solutions	The proposed solution should be offered for 1000 (One thousand) endpoints and shall be an on premise EDR or SaaS solutions Remarks: We request the department to modify the clause for larger vendor participation.	Not Agreed
180	Page 170, 3.7.5 Server Security	The proposed solution should be on-premises solution but will protect all types of servers (physical, virtual, cloud) from a single console.	The proposed solution's console should be on SaaS / on-premises solution but will protect all type of server (physical, virtual, cloud) from a single console. Remarks: We request the department to modify the clause for larger vendor participation.	Not Agreed
181	Page 170, 3.7.5 Server Security	The proposed server security solution has Antimalware, Application & device control, Web reputation, Host based firewall Host-based intrusion prevention solution (HIPS)/behavior analysis, Integrity monitoring, log inspection module along	The proposed server security solution has Anti-malware, Application/device control, Web reputation/FQDN based blocking websites, Host based firewall Host based intrusion prevention solution (HIPS)/behavior analysis, Integrity monitoring, log inspectionmodule along with sandbox integration in the same single agent.	Refer to Addendum No.1 of RFP Document

BCC
ICT Division
Enhancing Digital Government & Economy Project

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		with sandbox integration in the same single agent.	Remarks: We request the department to modify the clause for larger vendor participation.	

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
182	Page 170, 3.7.5 Server Security	Provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.	Provide protection of the vulnerable systems from malicious activities. Remarks: This clause is specific to a vendor. There is no need for virtual patching with new age AI/ML based solutions.	The requirement to "Provide virtual protection which shields vulnerable systems that are awaiting a security patch" is intended to ensure rapid protection of critical systems from known vulnerabilities during the window between vulnerability discovery and actual patch deployment. This does not specifically mandate a particular vendor's solution but reflects a widely recognized security practice such as virtual patching or equivalent mechanisms. The objective is to prevent exploitation during the patch management cycle.

8

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
183	Page 170, 3.7.5 Server Security	(1) Solution should track changes to critical Windows system files, registry keys and start-up folders, with no manual rule configuration needed(2) File integrity monitoring should monitor additions, deletions and changes to critical Windows system files, as an additional layer of security(3) Administrator can easily add additional monitoring locations (and exclusions) via policy in central dashboard, including files, folders registry keys and registry's.	Please remove these terms. Remarks: This change request seeks to remove references to File Integrity Monitoring (FIM) from the published feature sets, as this functionality is not universally integrated across server or endpoint security solutions from prominent OEMs. Currently, only one specific OEM offers few FIM feature sets like published one as a bundled feature, and seeking considerations on removing this exception.	The inclusion of File Integrity Monitoring (FIM) in the technical requirements is intended to strengthen endpoint and server security by ensuring visibility into unauthorized or unexpected changes to critical system components. This requirement aligns with globally accepted best practices for endpoint protection, especially in sensitive or regulated environments. The department acknowledges that the level of FIM integration may vary among vendors and solutions. However, the requirement does not limit acceptable solutions to a specific OEM. Solutions that provide equivalent capabilities whether natively, via integrated modules, or through interoperable

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				components will be considered compliant. Therefore, the FIM-related requirements will remain unchanged to preserve the intended security posture. Vendors may fulfill these requirements through native features, integrated modules, or through demonstrably interoperable solutions that meet the outlined objectives. If vendors propose alternative approaches to achieve the same security outcomes, they must clearly articulate how their solution addresses these needs within the technical proposal.
184	Page not found, 3.7.9 Network Behavior	(Not specified)	Proposed Solution should support data retention for minimum 30 Days	Please refer query response number 151

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Analysis (NBA) with Sandboxing		Remarks: Log retention or data retention period is not mentioned. Requesting to include minimum 30 days of data retention	
185	Page 55, 1.3 Key Personnel Team leader (1 person)	Bachelor's degree with 10 years' experience ofworking in a leadership role in designing anddeploying a country level information system and 5 years' experience of deploying Cloud/VirtualizationComputing platforms for large organizations.	Please change these terms. Remarks: Bachelor's degree with 5 years' experience ofworking in a leadership role in designing anddeploying a country level information system and 3years' experience of deploying Cloud/VirtualizationComputing platforms for large organizations.	Not Agreed
186	Page 56, 1.3 Key Personnel SOC Operations and Governance Specialist (1 person)	Bachelor's degree with 5 years' experience in SOC operations, governance, monitoring, and reporting frameworks. Experience working with SOC procedures, escalation matrixes, and ITSM/ticketingsystem integration sis highly preferred.		Not Agreed
187	Page 56, 1.3 Key Personnel Cyber Threat Intelligence Expert (1 person)	Bachelor's degree with 6 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or equivalent). Experience in external attack surface management solutions is a plus.	Please change these terms. Remarks: Bachelor's degree with 3 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or equivalent). Experience in external attack surface management solutions is a plus.	Not Agreed
188	Page 56, 1.3 Key Personnel	Bachelor's degree with 5 years' experience in SIEM (e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development.	Please change these terms.	Not Agreed

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	SIEM & SOAR Platform Expert (1 person)	Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred.	Remarks: Bachelor's degree with 3 years' experience in SIEM(e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development. Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred..	
189	Page 56, 1.3 Key Personnel SIEM & SOAR Platform Incident Response & Malware Analysis Expert (1 person)	Bachelor's degree with 5 years' experience in cybersecurity incident response, malware analysis (sandboxing – both online and on-premise), and digital forensics. Preferred certifications include GCFA,GCIH, or CHFI.	Please change these terms. Remarks: Bachelor's degree with 3 years' experience in cybersecurity incident response, malware analysis(sandboxing – both online and on premise), and digital forensics. Preferred certifications include GCFA, GCIH, or CHFI	Not Agreed
190	Page 56, 1.3 Key Personnel Network and Firewall Security Specialist (1 person)	Bachelor's degree with 5 years' experience in managing enterprise networks, deploying NGFWs(multiple types), VPNs, IDS/IPS. Certifications such asCCNP Security or Fortinet NSE4–7 are preferred.	Remarks: Bachelor's degree with 3 years' experience inmanaging enterprise networks, deploying NGFWs(multiple types), VPNs, IDS/IPS. Certifications such asCCNP Security or Fortinet NSE4–7 are preferred.	Not Agreed
191	Page 56, 1.3 Key Personnel Endpoint and Server Security Specialist (1 person)	Bachelor's degree with 5 years' experience in endpointdetection and response (EDR), server security, and privileged access management (PAM) systems.Relevant certifications like ECSA or OSCP are desirable.	Remarks: Bachelor's degree with 3 years' experience in endpointdetection and response (EDR), server security, andprivileged access management (PAM) systems.Relevant certifications like ECSA or OSCP or Cpnet or Equivalent aredesirable	Not Agreed

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
192	Page 56, 1.3 Key Personnel Cloud and External Threat Monitoring Specialist (1 person)	Bachelor's degree with 5 years' experience in securingcloud environments, hybrid cloud monitoring, and external threat detection. Certifications such as CCSP or AWS Certified Security – Specialty are an advantage.	Remarks: Bachelor's degree with 3 years' experience in securingcloud environments, hybrid cloud monitoring, andexternal threat detection. Certifications such as CCSP or AWS Certified Security – Specialty are an advantage.	Not Agreed
193	Page 57, 1.4 Subcontractors/vendors/manufacturers Security Information and Event Management (SIEM)	• Must be operating in the local/ international market for three (3) years.• The product should have been implemented by Four (4) customer / organization	Remarks: • Must be operating in the local/ international market for three (3) years. • The product should have been implemented by Four (2) customer / organization	Not Agreed
194	Page 57, 1.4 Subcontractors/vendors/manufacturers Security Orchestration, Automation, and Response (SOAR)	Note: A list of at least 4 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.	Remarks: Note: A list of at least 2 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	Not Agreed
195	Page 57, 1.4 Subcontractors/vendors/manufacturers Privileged Access Management (PAM)			

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
196	Page 57, 1.4 Subcontractors/vendors/manufacturers Endpoint Detection and Response (EDR) Page 57, 1.4 Subcontractors/vendors/manufacturers Server Security			
197	Page 57, 1.4 Subcontractors/vendors/manufacturers Network Behavior Analysis (NBA) with Sandboxing			
198	Page 58, 1.4 Subcontractors/vendors/manufacturers External Attack SurfaceManagement			
199	Page 58, 1.4 Subcontractors/vendors/manufacturers Malware Analysis Sandbox (OnPremise)			

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
200	3.7.6 Next Generation Firewall for SOC Performance Requirement	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 10 Gbps enterprise mix throughput from single appliance - Minimum 6 Gbps Threat protection throughput from single appliance - Minimum 500,000 concurrent sessions per seconds - Minimum 4K VLANs	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 10 Gbps enterprise mix Firewall throughput from single appliance - Minimum 6 Gbps Threat protection throughput from single appliance - Minimum 500,000 concurrent sessions per seconds - Minimum 4K VLANs Remarks: Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	Please refer query response number 1
201	3.7.7 VPN Firewall for CII Integration Performance Requirement	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 20 Gbps enterprise mix throughput from single appliance - Minimum 15 Gbps Threat protection throughput from single appliance - Minimum 1 million concurrent sessions per seconds - Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 - Minimum 4K VLANs	- The firewall shall support at least 5 virtual firewall instance from day 1 - Minimum 20 Gbps enterprise mix Firewall throughput from single appliance - Minimum 15 Gbps Threat protection throughput from single appliance - Minimum 1 million concurrent sessions per seconds - Minimum 200 IPSec Tunnel support along with 100 User VPN support from day 1 - Minimum 4K VLANs Remarks: Please clarify, is this enterprise mix throughput means the firewall throughput or else, if yes, suggesting to mention that	Please refer query response number 2
202	3.7.10 Server Farm Switch	- Minimum 4x10 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port	- Minimum 4x100 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port	Please refer query response number 3

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Interface		Remarks: Please clarify, is the uplink requirements is correct or typo mistake, usualy all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	
203	3.7.10 Server Farm Switch Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - DoS attack defense - ARP attack defense, and - ICMP attack defense	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher functionality. Like Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Please refer query response number 4
204	3.7.12 Perimeter Switch for CII Integration Interface	- Minimum 4x10 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port	- Minimum 4x100 GE uplink Ports - Minimum 48x10/25 GE SFP downlink Ports - 1 Out of Band Management Port Remarks: Please clarify, is the uplink requirements is correct or typo mistake, usualy all vendor supposed to have 40G or 100G uplink while downlink port is of 10G or 25G	Please refer query response number 5

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
205	3.7.12 Perimeter Switch for CII Integration Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - DoS attack defense - ARP attack defense, and	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Please refer query response number 6

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
206	3.7.13 Access Switch for SOC Room and Management Switch Security Feature	- Spanning Tree Port Fast - Root Guard - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense	- Spanning Tree Port Fast or Similar - Root Guard or Similar - Storm control (multicast and broadcast) - Link-level flow control (IEEE 802.3x) - The proposed equipment should support CPU defense - ARP attack defense, and - ICMP attack defense Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher funtionality. Like Other Vendors Supports STP Edged-port which is similar to Spanning Tree Port Fast and supports Root Protection which is similar to Root Guard	Please refer query response number 7
207	3.7.13 Access Switch for SOC Room and Management Management	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow or Similar Remarks: Vendor specific Proprietary protocols whereas other vendor support standard protocols which can provide similar or higher functionality	Please refer query response number 8
208	Page , 3.7.1 Security Information and Event Management (SIEM) (Log Collection or Ingestion Capabilities)	The proposed solution shall support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture with a 3rd party packet capture solution where required.	Partial Change Request: Reuest to remove "full packet capture with a 3rd party packet capture solution where required" Remarks Full Packet Capture is not part of SIEM solution	Please refer query response number 66

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
209	3.7.2 Security Orchestration, Automation, and Response (SOAR) (Threat Intelligence Integration)	The EDR should allow for custom IOC import and management (SHA-1, SHA-256 hashes, IP addresses, domains, URLs, YARA rules).	Request to change as "The EDR should allow for custom IOC import and management (SHA-1, SHA-256 hashes, IP addresses, domains, URLs, YARA rules) through Threat intel Feed coonector supported STIX/TAXII feed"	Please refer query response number 67
210	3.7.2 Security Orchestration, Automation, and Response (SOAR) (False Positive Management)	The solution should provide tools for exception management with approval workflows.	Request to change as "The solution should provide tools for exception management"	Refer to Addendum No. 29.
211	3.7.2 Security Orchestration, Automation, and Response (SOAR) (Response and Remediation Capabilities)	The solution must provide rollback capabilities for automated actions when appropriate.	Request to change as "The solution must support reversing persistent changes and restoring the system to its previous state"	Please refer query response number 69
212	3.7.2 Security Orchestration, Automation, and Response (SOAR) (Response and Remediation Capabilities)	The solution must support live response capabilities with minimal latency (<5 seconds).	Request to change as "The solution must support live response capabilities with minimal latency" Remarks Latency depends on varius factor specially endpoint CPU, RAM, no of running process.	Please refer query response number 70

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
213	3.7.2 Security Orchestration, Automation, and Response (SOAR) (Response and Remediation Capabilities)	The solution must enable system remediation actions including forced log-off, restart, or shutdown.	Request to change as "The solution must enable system remediation actions including Terminate process, Delete file, Clean persistent data, Block address on Firewall" Remarks The EDR remediation should be related to security action not to endpint system	Please refer query response number 71
214	3.7.2 Security Orchestration, Automation, and Response (SOAR) (Data Management and Compliance)	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	Request to change as "The EDR should include features or integrated with other tool like SIEM for compliance with HIPAA, PCI DSS, and other relevant regulations."	Please refer query response number 72
215	3.7.6 Next Generation Firewall for SOC (Qty. 02) (Next Generation Firewall Security Features)	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites.	Request to change as "The firewall should provide a URL category database with over 240 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites."	Please refer query response number 73

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
216	3.7.7 VPN Firewall for CII Integration (Qty. 02) (Next Generation Firewall Security Features)	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites.	Request to change as "The firewall should provide a URL category database with over 240 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites."	Please refer query response number 75
217	3.0.1: Network Behavior Analysis (NBA) with Sandboxing (Sandbox Environment)	The solution shall ensure process, registry, file system, network connection, and memory manipulation monitoring with API call analysis.	Change Request This is SIEM features and request to remove the line.	Refer to Addendum No. 1 of RFP Document.
218	3.0.1: Network Behavior Analysis (NBA) with Sandboxing (Integration Requirements)	The solution shall have support for STIX/TAXII and integration with threat intelligence platforms.	No as it can create issue with ML Change Request The solution shall have support for STIX/TAXII and integration with threat intelligence platforms or bidder shell quote threat Intel platform from day one.	Please refer query response number 78
219	3.0.1 External Attack Surface Management (Dashboard and Reporting)	The solution shall have feature to create template for custom report generation	Change Request	Please refer query response number 79

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			The solution shall have feature to filtered report by date range, keywords, categories, and relevance to security threat for report generation	
220	3.7.28 Malware Analysis Sandbox (On-premise) (Analysis Capabilities)	The solution must support pre- populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses.	Change Request The solution must support pre- populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses. Bidder will quote the all the nenessary license to run the system with full functionality from day one.	Please refer query response number 80
221	3.7.28 Malware Analysis Sandbox (On-premise) (Analysis Capabilities)	The solution shall have feature to add custom YARA and SIGMA rules to detect emerging malware	Yara is supported Change Request The solution shall have feature to add custom rule like YARA or SIGMA rules to detect emerging malware	Please refer query response number 81
222	3.7.28 Malware Analysis Sandbox (On-premise) (File and Protocol Support)	The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through inbuilt MTTM proxy.	Change Request The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through inbuilt MTTM proxy or integration of network security devices	Please refer query response number 82

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
223	3.7.28 Malware Analysis Sandbox (On-premise) (Integration and Reporting)	The proposed solution should have the ability to display the geo-location of identified command and control servers when possible.	Change Request The proposed solution should have the ability to display the geo-location of identified command and control servers with the help of network firewall when possible.	Please refer query response number 83
224	3.7.28 Malware Analysis Sandbox (On-premise) (Integration and Reporting)	The proposed solution should capture and store network traffic relevant to the analysis of detected threats, including packet captures (PCAPs).	Change Request Request to remove the line as it is a NDR features and NDR is quoting seperately. Remarks: NDR feature	Please refer query response number 84
225	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution shall support high availability, redundancy, and scalability.	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software and the solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on. Remarks: To make it more use case driven and useful to BCC NSOC. As SIEM consists of multiple modules, writing on high availability, redundancy and scalability supports are not enough.	Please refer query response number 133

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
226	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution must be software-based allowing flexible deployment models and architecture.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters. Remarks: To ensure reliability and reduce TCO. As SIEM consists of multiple modules, mentioning the detail deployment model is more suitable and it will be easier to understand the proposed solution	Please refer query response number 134
227	Page 148, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The solution shall support multi-tenancy from day 1 for separation of log ingestion, analysis, dashboard and reporting.	Please remove Remarks: Please help us understand that why in your environment a multi tenent solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 135

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
228	Page 148, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution shall support parsing single-line and multi-line log files.	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce TCO and make the solution reliable and always useful. Data parsers dependencies should be imposed to OEM for better efficiency	Please refer query response number 136
229	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing, normalization or filtering of data before ingestion into the system.	The proposed solution must comes with apps and add-ons for most common /well known security technologies and OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce the TCO and ensure availability of the parsers for any kind of data. Data parsers dependencies should be imposed to OEM for better efficiency	Please refer query response number 137

Digital Government & Economy Project ★ Enhancing
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
230	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time. Remarks: To make it more use case driven and useful to BCC NSOC, please change this clause as the change request	Please refer query response number 138
231	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks The solution shall support multiple correlation methods like Vulnerability, Signature, Statistical, Historical, Heuristic and Predictive correlation. The solution shall have pre-built correlation rules for rapid deployment and coverage of common attack scenarios.	The proposed solution must come with at least 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems and it should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.) The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques. Remarks: Request to change this as proposed. To ensure it covers all the attck scenarios and reliable and updated to most lastest known and unknown attacks.	Please refer query response number 139

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
232	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user. Remarks: Request to change this as proposed. To ensure the solution is robust and reduce the overall false positives greatly scientifically.	Please refer query response number 140
233	Page 150, 3.7.1 Security Information and Event Management (SIEM) (7. AI/ML and UEBA Capabilities)	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats. The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time. Investigate and respond to	Please refer query response number 141

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations. Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user. The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior. The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat. Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields. The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors. The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI. The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the	

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			correct sections of the chain. The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing. The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity. The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat. UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time. Note: Bidder must comply with all the mandatory points in the technical and functional requirement as mentioned above, Non-compliance with any of the mandatory requirements may make the bid liable for rejection. Also, please understand that any of the above technical requirements mentioned needs to be demonstrated as asked during the evaluation phase. Remarks: To ensure a right solution that is useful to BCC NSOC is available and not just for the namesake, please add the technical use case driven specifications of UBA.	

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
234	Page 150, 3.7.1 Security Information and Event Management (SIEM) (8. Integration Feature)	The solution shall support integration with any SOAR platform.	The solution shall support integration with any third party solution with in-built plug ins and apps and platform and must have SOAR solution from same OEM to reduce any complexity. Remarks: Request to change this as proposed. To ensure a end to end and seamless integration please rephrase	Please refer query response number 142
235	Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall provide pre-built SOC dashboards and have compliance-ready reports (PCI DSS, ISO 27001, NIST, GDPR).	The solution shall provide pre-built SOC dashboards like Security Posture, Incident Review and Executive Summary dashboard to help ivestigate fatser and Top officials have the SOC visibility. - The solution shall have compliance-ready reports, solution which can be configured modified as per need by the auditter by bidder. Remarks: Request to change this as proposed. To make it effective and use case driven please rephrase	Please refer query response number 143

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
236	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall support configuring separate dashboard for each tenant.	Please remove it Remarks: Please help us understand that why in your environment a multi tenant solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 144

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
237	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements. Remarks: Request to change this as proposed. To make sure it follows the standard process and less dependency and more coverage.	Please refer query response number 145

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
238	Page 152, 3.7.1 Security Information and Event Management (SIEM) (12. Licensing Option)	The supplier can offer any flexible and scalable licensing model based on the following baseline information: - Log Data Volume: 1500+ GB/day - EPS: 40,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value	Log Data Volume: 300+ GB/day - EPS: 8,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value Remarks: Requesting to please consider this proposed sizing. As all the CII will not be onboarded to the NSOC SIEM on day 1. So 1500 GB/day or 40,000 EPS are very high volume of data ingestion and will insure HUGE COST. As per our understanding, 300GB/day or 8,000 EPS should be sufficient for the operation. Kindly share the details of data sources for the right sizing of the solution for Day 1.	Please refer query response number 22
239	Page 152, 3.7.1 Security Information and Event Management (SIEM) (13. Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.	The offered solution shall be positioned either in the leader or Challengers quadrants for the last 5 consequtive years reports at Gartner Magic Quadrants for SIEM Remarks: Global Leaders for SIEM Solutions are listed in either Leaders or Challengers in the Gartner Magic Quadrant Reports. By adding Visionary will allow Startup solutions whose doesn't have much market references globally.	Please refer query response number 29

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
240	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (9. Integration)	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM Remarks: Request to change this as proposed. To ensure a end to end and seamless integration same OEM is cost effective	Please refer query response number 148
241	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (10. Licensing Option)	On-premise license for 50 analysts from day one and shall be scalable in the future.	0n premise license for 5 analysts from day one and shall be scalable in the future Remarks: Request to change this as proposed. 50 analysts licenses is too high for the NSOC requirement and insure HUGE COST. 5 analysts License should be enough considering 3 shifts operation as Licenses are concurrent in nature.	Please refer query response number 31

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
242	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE)	The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE). Remarks: Request to change this as proposed. Windows 7 and 8, Server 2012,2016,2019(regular) support has already been discontinued by Microsoft. So requesting to remove the end of life OS	Please refer query response number 150
243	Page N/A, 3.7.9 Network Behavior Analysis (NBA) with Sandboxing	**(Not specified)**	Proposed Solution should support data retention for minimum 30 Days Remarks: Log retention or data retention period is not mentioned. Requesting to include minimum 30 days of data retention	Please refer query response number 151
244	3.7.1 Security Information and Event Management (SIEM) "16 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4. Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1 No points will be awarded if no valid Gartner documentation is provided. Bidders	Change to "Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided.	Refer to Addendum No.1 of RFP Document

8

Enhancing Digital Government and Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Bidders must submit verifiable Gartner Magic Quadrant reports." Remarks: "Contradictory to clause 13 - Compliance. According to the Gartner Quadrant, Leaders & Visionaties are the similar product, and Challenger & Niche Player are similar. Only difference in Leadres & Visionaries are market cap of their products. On the other Global Report ""Critical Capabilities for SIEM"" from Gartner shows only the Leaders & Visionaries are the most capable products despite their market size.	
245	3.7.3 Privileged Access Management (PAM) "12 Access and Session Management"	The solution should have login security by limiting user login by parameters like originating IP address, terminal ID, type of login program or time of the day or geographical location etc. and limited concurrent login sessions by user.	Change to The solution should have login security by limiting user login by parameters like originating IP address, geographical location etc. and limited concurrent login sessions by user. Remarks: Users access PAM using web browser or desktop application and thus these requirements are invalid	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
246	3.7.3 Privileged Access Management (PAM) "18 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4. Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1. No points will be awarded if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Change to "Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports." Remarks: "Contradictory to another clause, 6 - General Features Solution must be from leaders quadrant of Gartner report for PAM"	Please refer to amendment Number: 3.

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
247	3.7.4. Endpoint Detection and Response (EDR) "5 Agent Deployment"	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE)	The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE). Remarks: Request to change this as proposed. Windows 7 and 8, Server 2012,2016,2019(regular) support has already been discontinued by Microsoft. So requesting to remove the end of life OS	Please refer to query response no: 150
248	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must provide configurable automated response actions including process termination, file quarantine, network isolation, and user session termination.	Change to The solution must provide configurable automated response actions including process termination, file quarantine, network isolation Remarks: EDR is an endpoint security solution which works from within the OS and cannot terminate the session, but it can isolate the affected device from the network.	Refer to Addendum No.1 of RFP Document
249	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The EDR should support the creation of custom response playbooks for specific detection scenarios. The solution must provide rollback capabilities for automated actions when appropriate. The EDR should support restoration of modified system files from trusted sources. The solution must include capabilities to restore the endpoint to a known good state after infection.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Refer to Addendum No.1 of RFP Document

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
250	3.7.4. Endpoint Detection and Response (EDR) "12 Management and Administration"	The EDR should include trend analysis for threat detection and system health metrics. The EDR should include a query language for custom data analysis and reporting. The solution must provide alert prioritization based on severity, confidence, and asset value. The EDR should support alert correlation to identify related security events. The solution must include alert assignment and tracking capabilities.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Refer to Addendum No.1 of RFP Document
251	3.7.4. Endpoint Detection and Response (EDR) "13 Integration Capabilities"	The EDR should enable bi-directional integration with SIEMs for alert synchronization. The EDR should support webhook capabilities for event-driven integrations. The solution must integrate with vulnerability management systems for risk correlation. The EDR should provide integrations with network security tools (firewalls, IPS/IDS). The solution must support integration with identity and access management systems. The solution must provide SOAR platform integration for orchestrated response actions. The EDR should support bidirectional communication with SOAR platforms.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Not Agreed. The specified integration capabilities including with SIEM, SOAR, identity and access management systems, vulnerability management tools, and network security devices are standard for

BCC
ICT Division
Enhancing Digital Government & Economy

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		The solution must expose all response actions through API for SOAR automation.		modern enterprise-grade EDR solutions, including on-premise deployments. These features are critical for achieving a unified cybersecurity posture, enabling automated threat response, and ensuring interoperability within an organization's existing security ecosystem. Leading on-premise EDR solutions support these integrations through APIs, webhooks, and plugin modules. Therefore, the requirements remain unchanged to ensure comprehensive

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				functionality and future scalability within a secured government infrastructure.
252	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should support tiered storage models for event data. The EDR should provide configurable purge policies while maintaining critical security events.	Delete	Not Agreed.
253	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	Change to The EDR should include features for compliance with PCI DSS, and other relevant regulations. Remarks: HIPAA Compliance is required for healthcare organizations only and irrelevant in this context	Please refer query response number 72
254	3.7.4. Endpoint Detection and Response (EDR) "18	The EDR should support horizontal scaling of server components. The solution must maintain performance under high event volume conditions.	Delete	Not Agreed.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Performance and Scalability"	The solution must provide estimated storage requirements based on endpoint count and retention periods. The EDR should optimize data storage through compression and deduplication. The EDR should provide tools for storage monitoring and capacity planning.		
255	3.7.6 Next Generation Firewall for SOC (Qty. 02) "11 Next Generation Firewall Security Features"	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites.	Change to The firewall should provide a URL category database with over 250 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites.	Please refer query response number 73
256	3.7.6 Next Generation Firewall for SOC (Qty. 02) "15 Warranty and Maintenance"	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 3 (three) business days.	Change to Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 30 (thirty) business days. Remarks: RMA requires atleast 30 Business Days	Please refer query response number 74

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
257	3.7.7 VPN Firewall for CII Integration (Qty. 02) "11 Next Generation Firewall Security Features"	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites.	Change to The firewall should provide a URL category database with over 250 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites.	Please refer query response number 75
258	3.7.7 VPN Firewall for CII Integration (Qty. 02) "15 Warranty and Maintenance"	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 3 (three) business days.	Change to Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 30 (thirty) business days. Remarks: RMA requires atleast 30 Business Days	Please refer query response number 76

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
259	3.7.9 Network Behavior Analysis (NBA) with Sandboxing "6 Network Behavior Analysis Capabilities"	The solution shall collect and analyze NetFlow/IPFIX/sFlow/jFlow, packet captures, logs from routers, switches, firewalls, DNS, DHCP, and authentication systems.	Delete Remarks: This requirement needs dedicated NDR soution which can be integrated with SIEM. No SIEM can do it out of the box without any type of additional NDA/NBA/network monitoring tool	The request is not accepted. Justification: This procurement package includes a Network Behavior Analysis (NBA) solution as part of the overall architecture.
260	3.7.10 Server Farm Switch (Qty. 4) "23 Warranty"	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts/device within maximum 3 (three) business days.	Change to Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 30 (thirty) business days. Rearks: RMA requires atleast 30 Business Days	The request is not accepted.
261	3.7.12 Perimeter Switch for CII Integration (Qty. 2) "23 Warranty"	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts/device within maximum 3 (three) business days.	Change to Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 30 (thirty) business days. Remarks: RMA requires atleast 30 Business Days	The request is not accepted.

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
262	**3.7.13 Access Switch for SOC Room and Management (Qty. 2) "23 Warranty"**	Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts/device within maximum 3 (three) business days.	Change to Comprehensive 3 years with 24 x 7 x 365 Technical Support & Assistance along with SLA of replacement of faulty parts within maximum 30 (thirty) business days. Remarks: RMA requires atleast 30 Business Days	The request is not accepted.
263	**3.7.24 Face & Fingerprint Time Attendance Access Control System "8 Wi-Fi"**	Wi-Fi must support dual-band (2.4 GHz and 5 GHz) for better stability	Change to Wi-Fi must support dual-band (2.4 GHz or 5 GHz) for better stability Remarks: Access Control runs on physical connection, 2.4 WiFi band enough for stability.	Refer to Addendum No.1 of RFP Document

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
264	**3.7.28 Malware Analysis Sandbox (On-premise) "4 Brief Description"**	An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux, Android), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure.	Change to An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure. Remarks: Scanning Android requires cloud which is contradictory with on-premise reuiqrement	The request is not accepted.

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
265	**3.7.28 Malware Analysis Sandbox (On-premise) "6 Performance Requirements"**	The system should be capable of analyzing files of size minimum 300 MB and more	Change to The system should be capable of analyzing files of size 30 MB and more Remarks: If the minimum file size should be 300 MB and smaller files are ignored, it will be vulnerable against attack since malicious files/malware are smaller file which are easier to propagate. Less that 1 MB file is the best choice for malware creators. If the file is 300 MB then it will be tough for distribution.	The system should be capable of analyzing files of any size upto 300 MB at least.
266	**3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"**	The sandbox must simulate hardware- level interactions and device drivers to provide a realistic execution environment for detecting evasive threats. The solution must support pre- populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses.	Delete	Please refer query response number 80

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
267	**3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"**	The solution shall have feature to add custom YARA and SIGMA rules to detect emerging malware	Change to The solution shall have feature to add custom YARA or SIGMA rules to detect emerging malware Remarks: One rule is sufficient since they works for same purpose	Please refer query response number 81
268	**3.7.28 Malware Analysis Sandbox (On-premise) "9 Integration and Reporting"**	The proposed solution should capture and store network traffic relevant to the analysis of detected threats, including packet captures (PCAPs).	Delete Remarks: PCAPs are required if the solution captures live packet but this requirement is for pure sandbox where the submitter needs to upload suspicious files for checking. No need to have PCAP.	Please refer query response number 84
269	**3.7.28 Malware Analysis Sandbox (On-premise) "10 Compliance and Data Protection"**	The solution OEM must have appropriate or attestations for relevant data protection laws (e.g., ISO 27001, SOC 2 Type II, GDRP etc.).	Delete Remarks: ISO 27001, SOC 2 Type II, GDRP etc. these are necessary certification for cloud based SOC	Refer to Addendum No.1 of RFP Document

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
270	**3.7.28 Malware Analysis Sandbox (On-premise) "13 Preferred: Malware Analysis Sandbox"**	Ability to host the solution in one or more hypervisor	Delete Remarks: Sandbox solutoins can be in different types like VM, appliance etc. Making them specific to hypervisor make the options limited	Refer to Addendum No.1 of RFP Document
271	Section III – Evaluation and Qualification Criteria 1.3.2 Average Annual Turnover Page 67	Minimum average annual turnover of US$ 4.0 million or equivalent amount, calculated as total certified payments received for contracts in progress or completed, in best three (3) within the last five (5) years from the Proposal submission date	Change to Minimum average annual turnover of US$ 3.5 million or equivalent amount, calculated as per yearly audit report, in best three (3) within the last five (5) years from the Proposal submission date	Refer to Addendum No.1 of RFP Document
272	Section III – Evaluation and Qualification Criteria 1.4.2 Specific Experience Page 69-71	"Participation as a prime supplier, management contractor, JV5 member, sub-contractor, with a minimum contract value US$ 3.0 million or equivalent amount under maximum two (2) similar contract(s) within the last five (5) years prior to the proposal submission deadline, that have been successfully and substantially completed and that are similar to the proposed Information System. The	Change to "Participation as a prime supplier, management contractor, JV5 member, sub-contractor, with a minimum contract value US$ 3.0 million or equivalent amount under maximum three (3) similar contract(s) within the last five (5) years prior to the proposal submission deadline, that have been successfully and substantially completed and that are similar to the proposed Information System. The contract will be	Refer to Addendum No.1 of RFP Document

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		contract will be treated as similar, if it includes any of the following components: Enterprise Security Tools (such as SIEM, SOAR, EASM), Enterprise Computing Hardware (e.g., servers, switches, firewalls, storage), Large-Scale Enterprise Software (e.g. Virtualization Software, ITSM), or any combination thereof, as described in Section VII Purchaser's Requirements for SOC/Network Operations Centers (NOC)/ Data Center (DC)/ Disaster Recovery (DR). The successfully completed similar contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s). The successful supply completion certificate issued by the Proposer's parent/subsidiary/sister/affiliate firm will not be considered for specific experience."	treated as similar, if it includes any of the following components: Enterprise Security Tools (such as SIEM, SOAR, EASM), Enterprise Computing Hardware (e.g., servers, switches, firewalls, storage), Large-Scale Enterprise Software (e.g. Virtualization Software, ITSM), or any combination thereof, as described in Section VII Purchaser's Requirements for SOC/Network Operations Centers (NOC)/ Data Center (DC)/ Disaster Recovery (DR). The successfully completed similar contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s). The successful supply completion certificate issued by the Proposer's parent/subsidiary/sister/affiliate firm will not be considered for specific experience."	
273	ITP 17.2	The Proposer must not propose Recurrent Cost Items	Clarification All the major software's are subscription based, need more clarification of the clause.	Please refer to Section VII – Requirements of the Information System in the RFP Document, which outlines the supply of major software in both the Implementation

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				Schedule Table and the System Inventory Table (under Supply and Installation Cost Items). The proposer will submit their proposal as per proposed solution licensing modality.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
276	3.7.1 Security Information and Event Management (SIEM) "16 "Log Collection or Ingestion Capabilities"	The proposed solution shall support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture with a 3rd party packet capture solution where required.	Change to The proposed solution shall integrate with a 3rd party packet capture solution to support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture where required.	Please refer query response number 66
277	3.7.1 Security Information and Event Management (SIEM) "16 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4.	Change to: Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years.	Please refer query response number 244.

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1 No points will be awarded if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports. Remarks: Contradictory to clause 13 - Compliance. According to the Gartner Quadrant, Leaders & Visionaties are the similar product, and Challenger & Niche Player are similar. Only difference in Leadres & Visionaries are market cap of their products. On the other Global Report "Critical Capabilities for SIEM" from Gartner shows only the Leaders & Visionaries are the most capable products despite their market size.	

8

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
278	3.7.3 Privileged Access Management (PAM) "12 Access and Session Management"	The solution should have login security by limiting user login by parameters like originating IP address, terminal ID, type of login program or time of the day or geographical location etc. and limited concurrent login sessions by user.	Change to The solution should have login security by limiting user login by parameters like originating IP address, geographical location etc. and limited concurrent login sessions by user. Remarks: Users access PAM using web browser or desktop application and thus these requirements are invalid	Please refer query response number 245
279	**3.7.3 Privileged Access Management (PAM)** ""13 Remote Users Management" "	Solution must have feature to handle the remote users and provide them access for target machines in secure manner without any need of any VPN solution and without exposing PIM infrastructure over internet.	Please explain remote users, their connectivity and location	The solution should provide secure connectivity via modern, integrated mechanisms such as secure gateways, brokers, encrypted tunnels, or equivalent technologies that do not require VPN client installations or direct internet exposure of privileged management infrastructure.

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
280	**3.7.3 Privileged Access Management (PAM)** ""13 Remote Users Management"	Solution must have biometric and password less authentication feature for remote users	This reqiures additional module (e.g. HSM) which customer needs to provide. Please share the brand/model so that we can confirm integration	Refer to Addendum No.1of RFP Document.
281	**3.7.3 Privileged Access Management (PAM)** "14 Threat Analytics and real-time response" "	Solution must be having features like artificial intelligence, Self learning and UBA (User Based Analytics) so that it can trigger a real-time alert in case of any unusual behavior of user or anomalous activities.	Machine learning based UBA requires cloud for analysis. Is cloud acceptable in this scenario? Secondly, UBA is already a part of SIEM. Do you need additional UBA?	Not Agreed.
282	**3.7.3 Privileged Access Management (PAM)** "14 Threat Analytics and real-time response"	Solution must able to identify Risky SPN (service principal name).Privileged accounts with SPN configuration can be vulnerable to offline brute-forcing and dictionary attacks, allowing a malicious insider to recover the account's clear-text password.	Deete Not a PAM feature	Not Agreed. similar solution can be offered by bidder that can ensure detection of malicious insider trying to recover the clear-text password of any account.

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
283	**3.7.3 Privileged Access Management (PAM)** "18 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4. Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1. No points will be awarded if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Change to "Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports." Remarks: "Contradictory to another clause, 6 - General Features Solution must be from leaders quadrant of Gartner report for PAM"	Please refer to query response Number: 246.

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
284	3.7.4. Endpoint Detection and Response (EDR) "5 Agent Deployment"	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE).	Change to The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2016/2019/2022+), macOS (11+) Remarks: EDR is a relatively new technology and supports only latest operting systems. Also, EDR is mostly designed for end user. Servers performs complex tasks and thus require dedicated server security which is another item in the RFP and major Linux distributors are covered there	Please refer query response number 150
285	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must provide configurable automated response actions including process termination, file quarantine, network isolation, and user session termination.	Change to The solution must provide configurable automated response actions including process termination, file quarantine, network isolation Remarks: EDR is an endpoint security solution which works from within the OS and cannot terminate the session, but it can isolate the affected device from the network.	Please refer query response number 248

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
286	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The EDR should support the creation of custom response playbooks for specific detection scenarios.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 249
287	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must provide rollback capabilities for automated actions when appropriate.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 69.
288	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The EDR should support restoration of modified system files from trusted sources.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	The clause "The EDR should support restoration of modified system files from trusted sources" was intended to enhance system recovery and integrity protection by allowing the restoration of critical files altered during an attack.

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
289	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must include capabilities to restore the endpoint to a known good state after infection.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer to response no: 249
290	3.7.4. Endpoint Detection and Response (EDR) "12 Management and Administration"	The EDR should include trend analysis for threat detection and system health metrics. The EDR should include a query language for custom data analysis and reporting. The solution must provide alert prioritization based on severity, confidence, and asset value. The EDR should support alert correlation to identify related security events. The solution must include alert assignment and tracking capabilities.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Please refer query response number 250

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
291	3.7.4. Endpoint Detection and Response (EDR) "13 Integration Capabilities"	The EDR should enable bi-directional integration with SIEMs for alert synchronization. The EDR should support webhook capabilities for event-driven integrations. The solution must integrate with vulnerability management systems for risk correlation. The EDR should provide integrations with network security tools (firewalls, IPS/IDS). The solution must support integration with identity and access management systems. The solution must provide SOAR platform integration for orchestrated response actions. The EDR should support bidirectional communication with SOAR platforms. The solution must expose all response actions through API for SOAR automation.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Please refer query response number 251

NR

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
292	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should support tiered storage models for event data. The EDR should provide configurable purge policies while maintaining critical security events.	Delete	Please refer query response number 252
293	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	Change to The EDR should include features for compliance with PCI DSS, and other relevant regulations. Remarks: HIPAA Compliance is required for healthcare organizations only and irrelevant in this context	Please refer query response number 72

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
294	3.7.4. Endpoint Detection and Response (EDR) "18 Performance and Scalability"	The EDR should support horizontal scaling of server components. The solution must maintain performance under high event volume conditions. The solution must provide estimated storage requirements based on endpoint count and retention periods. The EDR should optimize data storage through compression and deduplication. The EDR should provide tools for storage monitoring and capacity planning.	Delete	Please refer query response number 254
295	3.7.6 Next Generation Firewall for SOC (Qty. 02) "11 Next Generation Firewall Security Features"	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites.	Change to The firewall should provide a URL category database with over 250 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites.	Please refer query response number 73

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
296	3.7.9 Network Behavior Analysis (NBA) with Sandboxing "6 Network Behavior Analysis Capabilities"	The solution shall collect and analyze NetFlow/IPFIX/sFlow/jFlow, packet captures, logs from routers, switches, firewalls, DNS, DHCP, and authentication systems.	Delete Remarks: This requirement needs dedicated NDR soution which can be integrated with SIEM. No SIEM can do it out of the box without any type of additional NDA/NBA/network monitoring tool	Please refer query response number 259
297	3.7.14 Virtualization Software "4 Virtualization Platform Feature"”	The core virtualization software shall be based on linux kernel and support both VM and container	Delete Commercial virtualization software doesn’t open their karnel to edit, hence to use of mentioning the karnel preference.	It is asked to be based on Linux Kernel, not asked to be open. Commercial vendor can close virtualization software on the modified linux kernel.
298	3.7.22 Video Wall System “Resolution”	at least 4K (3840x2160)	Change to min 1080P per display	Please refer query response number 88
299	3.7.22 Video Wall System “Brightness”	700 cd/m² minimum	Change to Min. 500 cd/m²	Refer to Addendum No.1 of RFP Document.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
300	3.7.24 Face & Fingerprint Time Attendance Access Control System "8 Wi-Fi"	Wi-Fi must support dual-band (2.4 GHz and 5 GHz) for better stability	Change to Wi-Fi must support dual-band (2.4 GHz or 5 GHz) for better stability Remarks: Access Control runs on physical connection, 2.4 WiFi band enough for stability.	Please refer query response number 263
301	3.7.28 Malware Analysis Sandbox (On-premise) "4 Brief Description"	An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux, Android), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure.	Change to An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure. Remarks: Scanning Android requires cloud which is contradictory with on-premise reuiqrement	Please refer query response number 264

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
302	3.7.28 Malware Analysis Sandbox (On-premise) "6 Performance Requirements"	The system should be capable of analyzing files of size minimum 300 MB and more	Change to The system should be capable of analyzing files of size 30 MB and more Remarks: If the minimum file size should be 300 MB and smaller files are ignored, it will be vulnerable against attack since malicious files/malware are smaller file which are easier to propagate. Less that 1 MB file is the best choice for malware creators. If the file is 300 MB then it will be tough for distribution.	Please refer query response number 265
303	3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"	The sandbox must simulate hardware-level interactions and device drivers to provide a realistic execution environment for detecting evasive threats. The solution must support pre- populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses.	Delete	Please refer query response number 80
304	3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"	The solution shall have feature to add custom YARA and SIGMA rules to detect emerging malware	Change to The solution shall have feature to add custom YARA or SIGMA rules to detect emerging malware Remarks: One rule is sufficient since they works for same purpose	Please refer query response number 81

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
305	3.7.28 Malware Analysis Sandbox (On-premise) "9 Integration and Reporting"	The proposed solution should capture and store network traffic relevant to the analysis of detected threats, including packet captures (PCAPs).	Delete Remarks: PCAPs are required if the solution captures live packet but this requirement is for pure sandbox where the submitter needs to upload suspicious files for checking. No need to have PCAP.	Please refer query response number 84
306	3.7.28 Malware Analysis Sandbox (On-premise) "10 Compliance and Data Protection"	The solution OEM must have appropriate or attestations for relevant data protection laws (e.g., ISO 27001, SOC 2 Type II, GDRP etc.).	Delete Remarks: ISO 27001, SOC 2 Type II, GDRP etc. these are necessary certification for cloud based SOC	Please refer query response number 269
307	3.7.28 Malware Analysis Sandbox (On-premise) "13 Preferred: Malware Analysis Sandbox"	Ability to host the solution in one or more hypervisor	Delete Remarks: Sandbox solutoins can be in different types like VM, appliance etc. Making them specific to hypervisor make the options limited	Please refer query response number 270
308	3.7.31 Installation & Implementation of NSOC System "5 System Integration"	All systems must be integrated under a centralized management platform. Ensure interoperability between SIEM, SOAR, PAM, EDR, and NBA. Enable unified logging, alerting, dashboarding, and automated response mechanisms.	Please clarify how centralized management platform should work.	All relevant tools shall be integrated together to act as NSOC central system using SOAR and IT Service

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				Management System
309	3.7.33 Service Level Agreement (SLA) Priority Level 1: Emergency/Urgent/Critical Business Impact	For each hour of delay in MTTR beyond the committed time, a compensation of 0.005% of the performance security will be applied, up to a maximum of 5%.	For each of the penalty clause what is it based on? Total Contract Value? Please explain.	The penalty is not directly based on the Total Contract Value (TCV), but rather on the Performance Security amount.
310	Implementation Schedule "A. IMPLEMENTATION SCHEDULE TABLE B. SITE TABLE(S)"		Please explain B. SITE TABLE(S)	The question is not clear.
311	Implementation Schedule A. IMPLEMENTATION SCHEDULE TABLE	The implementation part of assignment mentioned in this Request for Proposals must be completed within 20 (Twenty) 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.	In the RFP document under the clause, 3.7.31 Installation & Implementation of NSOC System, 9 Timeline it states that the implementation must be completed within 20 Weeks while XLS 3.7.31 stats the entire installation and implementation must be completed within 90 days. Which is the correct duration for implementation? Is there a possibility of proposing a different time frame for implementation?	Bidders are requested to adhere to the stated 20-week timeline in their proposals. Any proposal suggesting a different implementation duration must clearly justify the reason for

Digital Government & Economy Project ★ Enhancing
BCC
ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				deviation and demonstrate how it would not compromise the project's objectives or quality. Such proposals will be subject to evaluation on a case-by-case basis at the discretion of the procurement entity. For clarity and avoidance of confusion, Bidder should consider the 20-week period as the official timeline for implementation

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
312	Background and Informational Materials A. BACKGROUND	"0.2.2 Strategic Importance and Urgency Given the increasing sophistication of cyberattacks and the growing reliance on digital platforms for public service delivery, the establishment of the NSOC is a strategic priority for national security and digital governance. The NSOC will: • Strengthen resilience across critical information infrastructures (CIIs)"	The RFP doesn't mention how many CIIs need to be integrated initially How the logs will be collected from CIIs	~~At least 10 CIIs initially~~ Refer to Addendum No. 1 of RFP Document.
313	B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS 1.2 Business Function Requirements to be met by the National Security Operation Center (NSOC)	1.2.1.3 Threat Intelligence Management • Aggregation and correlation of threat intelligence feeds from internal and external sources. • Storage and classification of threat intelligence data using a structured taxonomy. • Sharing of relevant intelligence with trusted stakeholders.	In the RFP there is no requirement for proposing a Threat Intelligence Management Platform. Is this a current solution the authority owns or does the tenderer need to propose a TIP as part of the design?	Refer to Addendum No. 1 of RFP Document.
314	**C. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS2.3 System Integration with Existing Platforms**	2.3.1 The Supplier MUST perform the following Integration Services: • Establish secure, standards-based integration with the following (examples): o Identity and Access Management systems o External threat intelligence platforms	Please give the Brand/Product names of the listed?	Integration between offered tools.

Enhancing Digital Government & Economy Project
BCC
ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		o Logging and monitoring tools o Government reporting or dashboard systems		
315	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "1 Team leader (1 person)"	Bachelor's degree with 10 years' experience of working in a leadership role in designing and deploying country level information system and 5 years' experience of deploying Cloud/Virtualization Computing platforms for large organizations.	Change to Bachelor's degree with 10 years' experience of working in a leadership role in designing and deploying country level information system and 5 years' experience of deploying Cloud/Virtualization Computing/cyber security platforms for large organizations. PMP, CISSP or similar certification	Not Agreed
316	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "2 SOC Operations and Governance Specialist (1 person)""	Bachelor's degree with 5 years' experience in SOC operations, governance, monitoring, and reporting frameworks. Experience working with SOC procedures, escalation matrixes, and ITSM/ticketing system integrations is highly preferred.	Change to: Bachelor's degree with 3 years' experience in SOC operations, governance, monitoring, and reporting frameworks. Experience working with SOC procedures, escalation matrixes, and ITSM/ticketing system integrations is highly preferred.	Not Agreed
317	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "3	Bachelor's degree with 6 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or equivalent). Experience in external attack surface management solutions is a plus.	Change to Bachelor's degree with 5 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or **equivalent**). Experience in external attack surface management solutions is a plus.	Please refer to query response: 187

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Cyber Threat Intelligence Expert (1 person)"			
318	**"SECTION III - EVALUATION AND QUALIFICATION CRITERIA** **1.3 Key Personnel"** **"4** **SIEM & SOAR Platform Expert (1 person)"**	Bachelor's degree with 5 years' experience in SIEM (e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development. Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred.	Change to: Bachelor's degree with 3 years' experience in SIEM (e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development. Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred.	Please refer to query response: 188
319	**"SECTION III - EVALUATION AND QUALIFICATION CRITERIA** **1.3 Key Personnel"** **"5** **Incident Response & Malware Analysis Expert (1 person)"**	Bachelor's degree with 5 years' experience in cybersecurity incident response, malware analysis (sandboxing – both online and on-premise), and digital forensics. Preferred certifications include GCFA, GCIH, or CHFI.	Change to Bachelor's degree with 3 years' experience in cybersecurity incident response, malware analysis (sandboxing – both online and on-premise), and digital forensics. Preferred certifications include GCFA, GCIH, or CHFI or similar certificate	Not Agreed

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
320	**"SECTION III - EVALUATION AND QUALIFICATION CRITERIA** **1.3 Key Personnel"** **"6** **Network and Firewall Security Specialist (1 person)"**	Bachelor's degree with 5 years' experience in managing enterprise networks, deploying NGFWs (multiple types), VPNs, IDS/IPS. Certifications such as CCNP Security or Fortinet NSE4–7 are preferred.	Change to Bachelor's degree with 3 years' experience in managing enterprise networks, deploying NGFWs (multiple types), VPNs, IDS/IPS. Certifications such as CCNP Security or Fortinet NSE4–7 are preferred.	Not Agreed
321	**"SECTION III - EVALUATION AND QUALIFICATION CRITERIA** **1.3 Key Personnel"** **"7** **Endpoint and Server Security Specialist (1 person)"**	Bachelor's degree with 5 years' experience in endpoint detection and response (EDR), server security, and privileged access management (PAM) systems. Relevant certifications like ECSA or OSCP are desirable.	Change to Bachelor's degree with 3 years' experience in endpoint detection and response (EDR), server security, and privileged access management (PAM) systems. Relevant certifications like ECSA, OSCP or similar certification on endpoint security	Not Agreed

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
322	**"SECTION III - EVALUATION AND QUALIFICATION CRITERIA** **1.3 Key Personnel"** **"8** **Cloud and External Threat Monitoring Specialist (1 person)"**	Bachelor's degree with 5 years' experience in securing cloud environments, hybrid cloud monitoring, and external threat detection. Certifications such as CCSP or AWS Certified Security – Specialty are an advantage.	Change to Bachelor's degree with 3 years' experience in securing cloud environments, hybrid cloud monitoring, and external threat detection. Certifications such as CCSP, AWS or similar cretification – Specialty are an advantage.	Not Agreed

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
325	ITP 17.2	The Proposer must not propose Recurrent Cost Items	Clarification All the major software's are subscription based, need more clarification of the clause.	Please refer to Section VII – Requirements of the Information System in the RFP Document, which outlines the supply of major software in both the Implementation Schedule Table and the System Inventory Table (under Supply and Installation Cost Items).

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
				The proposer will submit their proposal as per proposed solution licensing modality.
326	ITP 32.2	The weighting to be given for Rated Criteria (including technical and non-price factors) is: 40%. 1 Preliminary Project Plan addressing the required topics. 20% 2 Cyber security management strategies and implementation plans 10% 3 Preferred: EASM Feature 10% 4 Preferred: Malware Analysis Sandbox 10% 5 Security Information and Event Management (SIEM) 25% 6 Privileged Access Management (PAM) 25% Total 100%	Change to The weighting to be given for Rated Criteria (including technical and non-price factors) is: 40%. 1 Preliminary Project Plan addressing the required topics. 10% 2 Cyber security management strategies and implementation plans 20% 3 Preferred: EASM Feature 5% 4 Preferred: Malware Analysis Sandbox 5% 5 Security Information and Event Management (SIEM) 20% 6 Security Orchestration, Automation, and Response (SOAR) 10% 7 EPP, EDR & Server Security 10% 8 Network Behavior Analysis (NBA) with Sandboxing 5% 9 Privileged Access Management (PAM) 15% Total 100% Remarks:	Not Agreed.

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			"Building national level SOC is complex & requires high-stakes implementation, where planning of the project cruitital for Security Management, Implementation and for Long-Term Operational Success NSOC consists of very in-depth integration & commissioning of many components, and process. Considering all we recommend following scoring of the solutions,"	
327		SOC project management organization	Change for better clarification The Bidder themselves should be or, be supported by a Global Experienced and Skilled Technology Company with the experience & skill set of Designing, Managing & Implemention of National Level SOC Globally. Remarks: The RFP seems, it is a product procurement RFP, wheres Impelemnting NSOC is not only purchasing several product/solution for NSOC, but a lot of planning, management & coordination. Thus there should be an entity, who	Please refer query response number 275

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			will responsible and will do the lifting for such kind of management	
328	3.7.1 Security Information and Event Management (SIEM) "16 "Log Collection or Ingestion Capabilities"	The proposed solution shall support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture with a 3rd party packet capture solution where required.	Change to The proposed solution shall integrate with a 3rd party packet capture solution to support the collection of logs, flows (NetFlow, sFlow, IPFIX), and full packet capture where required.	Please refer query response number 66
329	3.7.1 Security Information and Event Management (SIEM) "16 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4. Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1 No points will be awarded if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Change to: Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports.	Please refer query response number 244

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: Contradictory to clause 13 - Compliance. According to the Gartner Quadrant, Leaders & Visionaties are the similar product, and Challenger & Niche Player are similar. Only difference in Leadres & Visionaries are market cap of their products. On the other Global Report "Critical Capabilities for SIEM" from Gartner shows only the Leaders & Visionaries are the most capable products despite their market size.	
330	3.7.3 Privileged Access Management (PAM) "12 Access and Session Management"	The solution should have login security by limiting user login by parameters like originating IP address, terminal ID, type of login program or time of the day or geographical location etc. and limited concurrent login sessions by user.	Change to The solution should have login security by limiting user login by parameters like originating IP address, geographical location etc. and limited concurrent login sessions by user. Remarks: Users access PAM using web browser or desktop application and thus these requirements are invalid	Please refer query response number 245

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
331	3.7.3 Privileged Access Management (PAM) ""13 Remote Users Management" "	Solution must have feature to handle the remote users and provide them access for target machines in secure manner without any need of any VPN solution and without exposing PIM infrastructure over internet.	Please explain remote users, their connectivity and location	Please refer query response number 279.
332	3.7.3 Privileged Access Management (PAM) ""13 Remote Users Management"	Solution must have biometric and password less authentication feature for remote users	This reqiures additional module (e.g. HSM) which customer needs to provide. Please share the brand/model so that we can confirm integration	Please refer query response number 280
333	3.7.3 Privileged Access Management (PAM) "14 Threat Analytics and real-time response"	Solution must be having features like artificial intelligence, Self learning and UBA (User Based Analytics) so that it can trigger a real-time alert in case of any unusual behavior of user or anomalous activities.	Machine learning based UBA requires cloud for analysis. Is cloud acceptable in this scenario? Secondly, UBA is already a part of SIEM. Do you need additional UBA?	Please refer query response number 281
334	3.7.3 Privileged Access Management (PAM) "14 Threat Analytics and real-time response"	Solution must able to identify Risky SPN (service principal name).Privileged accounts with SPN configuration can be vulnerable to offline brute-forcing and dictionary attacks, allowing a malicious insider to recover the account's clear-text password.	Deete Not a PAM feature	Please refer query response number 282

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
335	3.7.3 Privileged Access Management (PAM) "18 Preferred: Gartner Magic Quadrant-Based Product Evaluation"	Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products consistently ranked as a Leader in last two years will score 4. Products ranked as a Leader in last year will receive 3, Products ranked as a Challenger in last year will receive 2 and Products ranked as a Visionary in last year will receive 1. No points will be awarded if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports or excerpts for previous years to support their claims.	Change to "Bidders will be awarded 0 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category over the last two (2) consecutive years. Products ranked as a Leader will receive 10. Products ranked as a Visionary will receive 8. Bidder will be disqualified , if no valid Gartner documentation is provided. Bidders must submit verifiable Gartner Magic Quadrant reports." Remarks: "Contradictory to another clause, 6 - General Features Solution must be from leaders quadrant of Gartner report for PAM"	Please refer to query response Number: 246.
336	3.7.4. Endpoint Detection and Response (EDR) "5 Agent Deployment"	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE).	Change to The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2016/2019/2022+), macOS (11+) Remarks: EDR is a relatively new technology and supports only latest operting systems. Also, EDR is mostly	Please refer query response number 150

8

Enhancing Digital Government & Economy Project *
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			designed for end user. Servers performs complex tasks and thus require dedicated server security which is another item in the RFP and major Linux distributors are covered there	
337	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must provide configurable automated response actions including process termination, file quarantine, network isolation, and user session termination.	Change to The solution must provide configurable automated response actions including process termination, file quarantine, network isolation Remarks: EDR is an endpoint security solution which works from within the OS and cannot terminate the session, but it can isolate the affected device from the network.	Please refer query response number 248
338	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The EDR should support the creation of custom response playbooks for specific detection scenarios.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 249
339	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must provide rollback capabilities for automated actions when appropriate.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 69

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
340	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The EDR should support restoration of modified system files from trusted sources.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 288
341	3.7.4. Endpoint Detection and Response (EDR) "11 Response and Remediation Capabilities"	The solution must include capabilities to restore the endpoint to a known good state after infection.	Delete Remarks: These clauses are too product specific and not supported in most leading solutions	Please refer query response number 289
342	3.7.4. Endpoint Detection and Response (EDR) "12 Management and Administration"	The EDR should include trend analysis for threat detection and system health metrics. The EDR should include a query language for custom data analysis and reporting. The solution must provide alert prioritization based on severity, confidence, and asset value. The EDR should support alert correlation to identify related security events. The solution must include alert assignment and tracking capabilities.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Please refer query response number 250

Enhancing Digital Government & Economy Project
BCC
ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
343	3.7.4. Endpoint Detection and Response (EDR) "13 Integration Capabilities"	The EDR should enable bi-directional integration with SIEMs for alert synchronization. The EDR should support webhook capabilities for event-driven integrations. The solution must integrate with vulnerability management systems for risk correlation. The EDR should provide integrations with network security tools (firewalls, IPS/IDS). The solution must support integration with identity and access management systems. The solution must provide SOAR platform integration for orchestrated response actions. The EDR should support bidirectional communication with SOAR platforms. The solution must expose all response actions through API for SOAR automation.	Delete Remarks: These clauses are contradictory to the on-premsie EDR requirement which is mandatory for a government agency. Thus they need to be removed	Please refer query response number 251
344	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should support tiered storage models for event data. The EDR should provide configurable purge policies while maintaining critical security events.	Delete	Please refer query response number 252

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
345	3.7.4. Endpoint Detection and Response (EDR) "14 Data Management and Compliance"	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	Change to The EDR should include features for compliance with PCI DSS, and other relevant regulations. Remarks: HIPAA Compliance is required for healthcare organizations only and irrelevant in this context	Please refer query response number 72
346	3.7.4. Endpoint Detection and Response (EDR) "18 Performance and Scalability"	The EDR should support horizontal scaling of server components. The solution must maintain performance under high event volume conditions. The solution must provide estimated storage requirements based on endpoint count and retention periods. The EDR should optimize data storage through compression and deduplication. The EDR should provide tools for storage monitoring and capacity planning.	Delete	Please refer query response number 254
347	3.7.6 Next Generation Firewall for SOC (Qty. 02) "11 Next Generation Firewall Security Features"	The firewall should provide a URL category database with over 400 million URLs and accelerates access to specific categories of websites, improving access experience of high- priority websites.	Change to The firewall should provide a URL category database with over 250 million URLs and accelerates access to specific categories of websites, improving access experience of high-priority websites.	Please refer query response number 73

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
348	3.7.9 Network Behavior Analysis (NBA) with Sandboxing "6 Network Behavior Analysis Capabilities"	The solution shall collect and analyze NetFlow/IPFIX/sFlow/jFlow, packet captures, logs from routers, switches, firewalls, DNS, DHCP, and authentication systems.	Delete Remarks: This requirement needs dedicated NDR soution which can be integrated with SIEM. No SIEM can do it out of the box without any type of additional NDA/NBA/network monitoring tool	Please refer query response number 259
349	3.7.14 Virtualization Software "4 Virtualization Platform Feature""	The core virtualization software shall be based on linux kernel and support both VM and container	Delete Commercial virtualization software doesn't open their karnel to edit, hence to use of mentioning the karnel preference.	Please refer query response number 297
350	3.7.22 Video Wall System "Resolution"	at least 4K (3840x2160)	Change to min 1080P per display	Please refer query response number 88
351	3.7.22 Video Wall System "Brightness"	700 cd/m² minimum	Change to Min. 500 cd/m²	Please refer query response number 299

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
352	3.7.24 Face & Fingerprint Time Attendance Access Control System "8 Wi-Fi"	Wi-Fi must support dual-band (2.4 GHz and 5 GHz) for better stability	Change to Wi-Fi must support dual-band (2.4 GHz or 5 GHz) for better stability Remarks: Access Control runs on physical connection, 2.4 WiFi band enough for stability.	Please refer query response number 263
353	3.7.28 Malware Analysis Sandbox (On-premise) "4 Brief Description"	An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux, Android), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure.	Change to An on-premise Malware Analysis Sandbox is a locally deployed solution that safely analyzes suspicious files in a controlled environment, simulating real-world OS and application behavior to detect advanced threats. It supports large files, multiple formats, and platforms (Windows, Linux), provides deep behavioral insights, network traffic capture, and integrates with internal security tools—while ensuring data privacy, compliance, and full control within the organization's infrastructure. Remarks: Scanning Android requires cloud which is contradictory with on-premise reuiqrement	Please refer query response number 264

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
354	3.7.28 Malware Analysis Sandbox (On-premise) "6 Performance Requirements"	The system should be capable of analyzing files of size minimum 300 MB and more	Change to The system should be capable of analyzing files of size 30 MB and more Remarks: If the minimum file size should be 300 MB and smaller files are ignored, it will be vulnerable against attack since malicious files/malware are smaller file which are easier to propagate. Less that 1 MB file is the best choice for malware creators. If the file is 300 MB then it will be tough for distribution.	Please refer query response number 265
355	3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"	The sandbox must simulate hardware-level interactions and device drivers to provide a realistic execution environment for detecting evasive threats. The solution must support pre-populated licensed/activated copies of operating systems and applications (e.g. Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses.	Delete	Please refer query response number 80
356	3.7.28 Malware Analysis Sandbox (On-premise) "7 Analysis Capabilities"	The solution shall have feature to add custom YARA and SIGMA rules to detect emerging malware	Change to The solution shall have feature to add custom YARA or SIGMA rules to detect emerging malware	Please refer query response number 81

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: One rule is sufficient since they works for same purpose	
357	3.7.28 Malware Analysis Sandbox (On-premise) "9 Integration and Reporting"	The proposed solution should capture and store network traffic relevant to the analysis of detected threats, including packet captures (PCAPs).	Delete Remarks: PCAPs are required if the solution captures live packet but this requirement is for pure sandbox where the submitter needs to upload suspicious files for checking. No need to have PCAP.	Please refer query response number 84
358	3.7.28 Malware Analysis Sandbox (On-premise) "10 Compliance and Data Protection"	The solution OEM must have appropriate or attestations for relevant data protection laws (e.g., ISO 27001, SOC 2 Type II, GDRP etc.).	Delete Remarks: ISO 27001, SOC 2 Type II, GDRP etc. these are necessary certification for cloud based SOC	Please refer query response number 269
359	3.7.28 Malware Analysis Sandbox (On-premise) "13 Preferred: Malware Analysis Sandbox"	Ability to host the solution in one or more hypervisor	Delete Remarks: Sandbox solutoins can be in different types like VM, appliance etc. Making them specific to hypervisor make the options limited	Please refer query response number 270

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
360	3.7.31 Installation & Implementation of NSOC System "5 System Integration"	All systems must be integrated under a centralized management platform. Ensure interoperability between SIEM, SOAR, PAM, EDR, and NBA. Enable unified logging, alerting, dashboarding, and automated response mechanisms.	Please clarify how centralized management platform should work.	Please refer query response number 308
361	3.7.33 Service Level Agreement (SLA) Priority Level 1: Emergency/Urgent/Critical Business Impact	For each hour of delay in MTTR beyond the committed time, a compensation of 0.005% of the performance security will be applied, up to a maximum of 5%.	For each of the penalty clause what is it based on? Total Contract Value? Please explain.	The penalty is not directly based on the Total Contract Value (TCV), but rather on the Performance Security amount.
362	Implementation Schedule "A. IMPLEMENTATION SCHEDULE TABLE B. SITE TABLE(S)"		Please explain B. SITE TABLE(S)	Please refer query response number 310.
363	Implementation Schedule A. IMPLEMENTATION SCHEDULE TABLE	The implementation part of assignment mentioned in this Request for Proposals must be completed within 20 (Twenty) 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	In the RFP document under the clause, 3.7.31 Installation & Implementation of NSOC System, 9 Timeline it states that the implementation must be completed within 20 Weeks while XLS 3.7.31 stats the entire installation and implementation must be completed within 90 days.	Please refer query response number 311

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		be provided in detail with clear separation of duties.	Which is the correct duration for implementation? Is there a possibility of proposing a different time frame for implementation?	
364	Background and Informational Materials A. BACKGROUND	"0.2.2 Strategic Importance and Urgency Given the increasing sophistication of cyberattacks and the growing reliance on digital platforms for public service delivery, the establishment of the NSOC is a strategic priority for national security and digital governance. The NSOC will: • Strengthen resilience across critical information infrastructures (CIIs)"	The RFP doesn't mention how many CIIs need to be integrated initially How the logs will be collected from CIIs	Please refer query response number 312
365	B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS 1.2 Business Function Requirements to be met by the National Security Operation Center (NSOC)	1.2.1.3 Threat Intelligence Management • Aggregation and correlation of threat intelligence feeds from internal and external sources. • Storage and classification of threat intelligence data using a structured taxonomy. • Sharing of relevant intelligence with trusted stakeholders.	In the RFP there is no requirement for proposing a Threat Intelligence Management Platform. Is this a current solution the authority owns or does the tenderer need to propose a TIP as part of the design?	Please refer query response number 313

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
366	C. SERVICE SPECIFICATIONS – SUPPLY & INSTALL ITEMS 2.3 System Integration with Existing Platforms	2.3.1 The Supplier MUST perform the following Integration Services: • Establish secure, standards-based integration with the following (examples): o Identity and Access Management systems o External threat intelligence platforms o Logging and monitoring tools o Government reporting or dashboard systems	Please give the Brand/Product names of the listed?	Please refer query response number 314
367	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "1 Team leader (1 person)"	Bachelor's degree with 10 years' experience of working in a leadership role in designing and deploying country level information system and 5 years' experience of deploying Cloud/Virtualization Computing platforms for large organizations.	Change to Bachelor's degree with 10 years' experience of working in a leadership role in designing and deploying country level information system and 5 years' experience of deploying Cloud/Virtualization Computing/cyber security platforms for large organizations. PMP, CISSP or similar certification	Please refer query response number 315
368	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "2	Bachelor's degree with 5 years' experience in SOC operations, governance, monitoring, and reporting frameworks. Experience working with SOC procedures, escalation matrixes, and ITSM/ticketing system integrations is highly preferred.	Change to Bachelor's degree with 3 years' experience in SOC operations, governance, monitoring, and reporting frameworks. Experience working with SOC procedures, escalation matrixes,	Please refer query response number 316

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	SOC Operations and Governance Specialist (1 person)""		and ITSM/ticketing system integrations is highly preferred.	
369	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "3 Cyber Threat Intelligence Expert (1 person)"	Bachelor's degree with 6 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or equivalent). Experience in external attack surface management solutions is a plus.	Change to Bachelor's degree with 3 years' experience in Cyber Threat Intelligence (CTI), cyber threat hunting, and advanced threat correlation. Preferably certified (GCTI, CTIA, or equivalent). Experience in external attack surface management solutions is a plus.	Please refer query response number 187
370	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "4 SIEM & SOAR Platform Expert (1 person)"	Bachelor's degree with 5 years' experience in SIEM (e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development. Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred.	Change to Bachelor's degree with 3 years' experience in SIEM (e.g., Splunk, QRadar, ArcSight) deployment and SOAR playbook development. Experience integrating UEBA capabilities is desirable. SIEM/SOAR certifications are preferred.	Please refer query response number 188
371	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "5	Bachelor's degree with 5 years' experience in cybersecurity incident response, malware analysis (sandboxing – both online and on-premise), and digital forensics. Preferred certifications include GCFA, GCIH, or CHFI.	Change to Bachelor's degree with 3 years' experience in cybersecurity incident response, malware analysis (sandboxing – both online and on-premise), and digital forensics.	Please refer query response number 319

Enhancing Digital Government & Economy Project
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Incident Response & Malware Analysis Expert (1 person)"		Preferred certifications include GCFA, GCIH, or CHFI or similar certificate	
372	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "6 Network and Firewall Security Specialist (1 person)"	Bachelor's degree with 5 years' experience in managing enterprise networks, deploying NGFWs (multiple types), VPNs, IDS/IPS. Certifications such as CCNP Security or Fortinet NSE4–7 are preferred.	Change to Bachelor's degree with 3 years' experience in managing enterprise networks, deploying NGFWs (multiple types), VPNs, IDS/IPS. Certifications such as CCNP Security or Fortinet NSE4–7 are preferred.	Please refer query response number 320
373	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "7 Endpoint and Server Security Specialist (1 person)"	Bachelor's degree with 5 years' experience in endpoint detection and response (EDR), server security, and privileged access management (PAM) systems. Relevant certifications like ECSA or OSCP are desirable.	Change to Bachelor's degree with 3 years' experience in endpoint detection and response (EDR), server security, and privileged access management (PAM) systems. Relevant certifications like ECSA, OSCP or similar certification on endpoint security	Please refer query response number 321
374	"SECTION III - EVALUATION AND QUALIFICATION CRITERIA 1.3 Key Personnel" "8	Bachelor's degree with 5 years' experience in securing cloud environments, hybrid cloud monitoring, and external threat detection. Certifications such as CCSP or AWS Certified Security – Specialty are an advantage.	Change to Bachelor's degree with 3 years' experience in securing cloud environments, hybrid cloud monitoring, and external threat detection. Certifications such as CCSP,	Please refer query response number 322

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Cloud and External Threat Monitoring Specialist (1 person)"		AWS or similar cretification – Specialty are an advantage.	

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
375	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution shall support high availability, redundancy, and scalability.	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software and the solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on. Remarks: To make it more use case driven and useful to BCC NSOC. As SIEM consists of multiple modules, writing on high availability, redundancy and scalability supports are not enough.	Please refer query response number 133
376	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution must be software-based allowing flexible deployment models and architecture.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling &	Please refer query response number 134

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			disabling should be available depending on the device, IP address, and other related parameters. Remarks: To ensure reliability and reduce TCO. As SIEM consists of multiple modules, mentioning the detail deployment model is more suitable and it will be easier to understand the proposed solution	
377	Page 148, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The solution shall support multi-tenancy from day 1 for separation of log ingestion, analysis, dashboard and reporting.	Please remove Remarks: Please help us understand that why in your environment a multi tenent solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 135

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
378	Page 148, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution shall support parsing single-line and multi-line log files.	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce TCO and make the solution reliable and always useful. Data parsers dependencies should be imposed to OEM for better efficiency	Please refer query response number 136
379	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing, normalization or filtering of data before ingestion into the system.	The proposed solution must comes with apps and ad-ons for most common /well known security technologies and OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	Please refer query response number 137

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: To reduce the TCO and ensure availability of the parsers for any kind of data. Data parsers dependencies should be imposed to OEM for better efficiency	
380	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time. Remarks: To make it more use case driven and useful to BCC NSOC, please change this clause as the change request	Please refer query response number 138
381	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks The solution shall support multiple correlation methods like Vulnerability, Signature, Statistical, Historical, Heuristic and Predictive correlation. The solution shall have pre-built correlation rules for rapid	The proposed solution must come with at least 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems and it should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.) The proposed solution should have Out of The	Please refer query response number 139

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
		deployment and coverage of common attack scenarios.	Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques. Remarks: Request to change this as proposed. To ensure it covers all the attck scenarios and reliable and updated to most lastest known and unknown attacks.	
382	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user. Remarks: Request to change this as proposed. To ensure the solution is robust and reduce the overall false positives greatly scientifically.	Please refer query response number 140

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
383	Page 150, 3.7.1 Security Information and Event Management (SIEM) (7. AI/ML and UEBA Capabilities)	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats. The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time. Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations. Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user. The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior. The proposed solution should have threat detection technique and models to distill anomalies	Please refer query response number 141

8

Enhancing Digital Government & Economy Project * BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat. Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields. The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors. The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI. The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain. The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing. The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity. The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

8

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time. Note: Bidder must comply with all the mandatory points in the technical and functional requirement as mentioned above, Non-compliance with any of the mandatory requirements may make the bid liable for rejection. Also, please understand that any of the above technical requirements mentioned needs to be demonstrated as asked during the evaluation phase. Remarks: To ensure a right solution that is useful to BCC NSOC is available and not just for the namesake, please add the technical use case driven specifications of UBA.	

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
384	Page 150, 3.7.1 Security Information and Event Management (SIEM) (8. Integration Feature)	The solution shall support integration with any SOAR platform.	The solution shall support integration with any third party solution with in-built plug ins and apps and platform and must have SOAR solution from same OEM to reduce any complexity. Remarks: Request to change this as proposed. To ensure a end to end and seamless integration please rephrase	Please refer query response number 142
385	Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall provide pre-built SOC dashboards and have compliance-ready reports (PCI DSS, ISO 27001, NIST, GDPR).	The solution shall provide pre-built SOC dashboards like Security Posture, Incident Review and Executive Summary dashboard to help ivestigate fatser and Top officials have the SOC visibility. - The solution shall have compliance-ready reports, solution which can be configured modified as per need by the auditter by bidder. Remarks: Request to change this as proposed. To make it effective and use case driven please rephrase	Please refer query response number 143

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
386	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall support configuring separate dashboard for each tenant.	Please remove it Remarks: Please help us understand that why in your environment a multi tenant solution is needed? Its typically required in a service provider's /MSSP environment where various tenants needs to be catered and billed from one single service provider, please remove the clause.	Please refer query response number 144
387	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements.	Please refer query response number 145

Digital Government & Economy Project ★ Enhancing
BCC
ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: Request to change this as proposed. To make sure it follows the standard process and less dependency and more coverage.	
388	Page 152, 3.7.1 Security Information and Event Management (SIEM) (12. Licensing Option)	The supplier can offer any flexible and scalable licensing model based on the following baseline information: - Log Data Volume: 1500+ GB/day - EPS: 40,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value	Log Data Volume: 300+ GB/day - EPS: 8,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value Remarks: Requesting to please consider this proposed sizing. As all the CII will not be onboarded to the NSOC SIEM on day 1. So 1500 GB/day or 40,000 EPS are very high volume of data ingestion and will insure HUGE COST. As per our understanding, 300GB/day or 8,000 EPS should be sufficient for the operation. Kindly share the details of data sources for the right sizing of the solution for Day 1.	Please refer query response number 22

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
389	Page 152, 3.7.1 Security Information and Event Management (SIEM) (13. Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.	The offered solution shall be positioned either in the leader or Challengers quadrants for the last 5 consequtive years reports at Gartner Magic Quadrants for SIEM Remarks: Global Leaders for SIEM Solutions are listed in either Leaders or Challengers in the Gartner Magic Quadrant Reports. By adding Visionary will allow Startup solutions whose doesn't have much market references globally.	Please refer query response number 29
390	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (9. Integration)	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM Remarks: Request to change this as proposed. To ensure a end to end and seamless integration same OEM is cost effective	Please refer query response number 148

Enhancing Digital Government & Economy Project ★ BCC ICT Division

Sl. No.	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
391	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (10. Licensing Option)	On-premise license for 50 analysts from day one and shall be scalable in the future.	0n premise license for 5 analysts from day one and shall be scalable in the future Remarks: Request to change this as proposed. 50 analysts licenses is too high for the NSOC requirement and insure HUGE COST. 5 analysts License should be enough considering 3 shifts operation as Licenses are concurrent in nature.	Please refer query response number 31
392	Page 163, 3.7.4 Endpoint Detection and Response (EDR) (5. Agent Deployment)	The EDR agent must support installation on multiple operating systems including Windows (7/8/10/11, Server 2012/2016/2019/2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE)	The EDR agent must support installation on multiple operating systems including Windows (10/11, Server 2022), macOS (10.13+), Linux (major distributions including RHEL, Ubuntu, CentOS, SUSE). Remarks: Request to change this as proposed. Windows 7 and 8, Server 2012,2016,2019(regular) support has already been discontinued by Microsoft. So requesting to remove the end of life OS	Please refer query response number 150
393	Page N/A, 3.7.9 Network Behavior Analysis (NBA) with Sandboxing	**(Not specified)**	Proposed Solution should support data retention for minimum 30 Days Remarks: Log retention or data retention period is not mentioned. Requesting to include minimum 30 days of data retention	Please refer query response number 151

Enhancing Digital Government & Economy Project * BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
394		Not Mentioned	Requesting to share the desired architecture as part of the RFP Remarks: ->The desired architecture will help to ensure all bidders to have a common understanding and enabling them to propose their financial offers on an equal basis. -> It will provide much-needed clarity in defining the SI/implementation scope, as integration is one of the most critical aspects of this national-level project. -> In a SOC solution, the architectural design holds greater importance than individual tools, as it forms the foundation for security, scalability, and operations. -> It is crucial to understand the planning for connecting all Critical Information Infrastructure (CII) organizations to the NSOC. The architecture will define how logs, alerts, and threat data from diverse entities are ingested, normalized, stored, and analyzed efficiently. This is essential for accurate and timely threat detection and response. -> This will significantly help in aligning proposal with the strategic vision of the NSOC project and in achieving the overall national security objectives.	As per the RFP, it is the responsibility of the bidder to propose a suitable end-to-end architecture that meets the functional, technical, and security requirements outlined in the bidding documents. The objective is to encourage innovative and context-aware solutions from qualified bidders, leveraging their domain expertise and global best practices. Bidders are expected to: Propose a scalable, secure, and modular architecture aligned with the strategic objectives of the NSOC. Demonstrate how their proposed architecture ensures efficient ingestion, normalization, storage, correlation, and analysis of logs and threat data from various Critical Information Infrastructure (CII) entities.

Enhancing Digital Government & Economy Project
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
395	3.7.4 Endpoint Detection and Response (EDR)Threat Intelligence Integration 227	The EDR should integrate with TAXII/STIX feeds for automated intelligence updates.	The EDR should integrate with threat intel feeds for automated intelligence updates. Remarks: Updating the requirement to “threat intel feeds” broadens compatibility beyond just TAXII/STIX formats, allowing integration with a wider range of intelligence sources. This flexibility ensures the EDR can ingest diverse, real-time threat data, enhancing detection and response capabilities. It future-proofs the solution against evolving threat feed standards.	Refer to Addendum No. 1 of RFP Document.
396	3.7.4 Endpoint Detection and Response (EDR) Response and Remediation Capabilities 227	The EDR should support the creation of custom response playbooks for specific detection scenarios.	The EDR should support the creation of custom response playbooks/Automation rule for specific detection scenarios. Remarks: Including “Automation rule” along expands the capability for automated, customizable incident responses. This enhances flexibility in tailoring detection scenario actions, enabling faster and more precise threat mitigation. It aligns with modern EDR functionality that combines playbooks and automation for improved operational efficiency.	Please refer query response number 249

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
397	3.7.4 Endpoint Detection and Response (EDR) Response and Remediation Capabilities 229	The solution must provide remote shell capabilities for incident investigation.	"The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below : -File hash Information collection -Termination of the service -Download of binary -Addition of hash value to block list -Delete the file -Send the hash to get the verdict (TI integration) -Execute a python script -Execute a powershell script" Remarks Including GUI-based remote response capabilities with features like live terminal access, script execution, file control, and threat intelligence integration ensures rapid, precise response to threats without needing full remote access or third-party tools. This reduces incident response time, improves analyst	No change to prevent vendors locking in.

8

Enhancing Digital Government & Economy Project
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			efficiency, and enables surgical remediation directly from the console.	
398	3.7.4 Endpoint Detection and Response (EDR) Management and Administration 231	The solution must support the export of reports in multiple formats (PDF, CSV, HTML).	The solution must support the export of reports in multiple formats (PDF, CSV). Remarks PDF and CSV—which are widely accepted for reporting and data analysis	No change.
399	3.7.4 Endpoint Detection and Response (EDR) Agent Deployment 224	The agent shall be lightweight and must be optimized to ensure minimal system resource utilization	Proposed solution must have unified agent for detection, prevention , response and forensics and it must be lightweighted. Agent size should be less than 60 Mb and solution must have mechanism to provide msi package out of the box. Remarks A unified, lightweight agent under 60 MB minimizes system resource usage while simplifying deployment and management across endpoints. Providing an MSI package out of the box ensures ease of integration with enterprise software deployment tools, enhancing scalability and reducing operational overhead during large-scale rollouts.	No change to prevent vendors locking in.
400	3.7.4 Endpoint Detection and Response (EDR)		Request to add	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project *
BCC
ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Data Management and Compliance 233		Proposed Solution must be in top 3 vendor in last 2 MITRE evaluations (Wizard Spider + Sandstrom & Turla). Remarks Requiring the solution to be in the top 3 of the last two MITRE evaluations ensures selection of a vendor with consistently strong performance against advanced threat groups. This reflects the solution's ability to deliver high detection accuracy, low false positives, and effective real-world threat coverage—critical for strengthening the organization's security posture.	
401	3.7.4 Endpoint Detection and Response (EDR) Data Management and Compliance 233		Request to add Proposed solution must have 99.9% detection rate in latest two MITRE evaluation without any modification and delayed detection. Remarks A 99.9% detection rate without modifications or delayed detection in MITRE evaluations demonstrates the solution's native effectiveness and reliability. This ensures that the product performs optimally out-of-the-box, offering faster threat identification and	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project
BCC
ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			reducing dependency on manual tuning—key for timely and accurate incident response.	
402	3.7.4 Endpoint Detection and Response (EDR) Data Management and Compliance 233		Request to add Proposed solution must provide 30 days of online retention for raw telemetry and 180 days of retention for alerts and incidents. Remarks Having 30 days of raw telemetry online allows for deep forensic investigations and threat hunting within a meaningful window. Retaining alerts and incidents for 180 days supports compliance, trend analysis, and correlation of long-term attack patterns, which is essential for effective security operations and incident response.	No change to prevent vendors locking in.
403	3.7.4 Endpoint Detection and Response (EDR) Threat Management 234		Request to add Proposed solution should able to submit unknown files by its own to sandbox without user/administrator intervention and it should support up to 1,000,000 verdict queries per day. Remarks	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Automatic submission of unknown files to sandboxing without user intervention ensures real-time analysis and zero-delay protection against emerging threats. Supporting up to 1,000,000 verdict queries per day guarantees scalability for large environments, enabling high-volume threat detection without bottlenecks or performance degradation.	
404	3.7.4 Endpoint Detection and Response (EDR) Threat Intelligence Integration 226		Request to add Proposed solution should have capability to search and destroy to swiftly sweep across endpoint and eradicate threats without any script Remarks Requiring a no-script search and destroy capability ensures even non-technical analysts can quickly locate and eliminate threats across all endpoints. This enhances operational efficiency, reduces response time, and minimizes the risk of human error, enabling consistent and scalable threat remediation.	No change to prevent vendors locking in.
405	3.7.4 Endpoint Detection and Response (EDR) Management and Administration 231		Request to add Proposed solution must provide encryption management for BitLocker and file vault, it must be part of unified agent.	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project * BCC ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks Native encryption management for BitLocker and FileVault within a unified agent streamlines data protection and compliance without requiring additional tools. This simplifies policy enforcement, reduces agent sprawl, and ensures consistent visibility and control over endpoint encryption across the organization.	
406	3.7.5 Server Security General Requirements 237		Request to add Proposed Solution must be in top 3 vendor in last 2 MITRE evaluations (Wizard Spider + Sandstrom & Turla). Remarks Requiring the solution to be in the top 3 of the last two MITRE evaluations ensures selection of a vendor with consistently strong performance against advanced threat groups. This reflects the solution's ability to deliver high detection accuracy, low false positives, and effective real-world threat coverage—critical for strengthening the organization's security posture.	No change to prevent vendors locking in.

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
407	3.7.5 Server Security General Requirements 237		Request to add Proposed solution must have 99.9% detection rate in latest two MITRE evaluation without any modification and delayed detection. Remarks A 99.9% detection rate without modifications or delayed detection in MITRE evaluations demonstrates the solution's native effectiveness and reliability. This ensures that the product performs optimally out-of-the-box, offering faster threat identification and reducing dependency on manual tuning—key for timely and accurate incident response.	No change to prevent vendors locking in.
408	3.7.5 Server Security General Requirements 237		Request to add Proposed solution must provide 30 days of online retention for raw telemetry and 180 days of retention for alerts and incidents. Remarks Having 30 days of raw telemetry online allows for deep forensic investigations and threat hunting within a meaningful window. Retaining alerts and incidents for 180 days supports compliance, trend analysis, and correlation of long-term attack patterns, which is essential for effective security operations and incident response.	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
409	3.7.5 Server Security General Requirements 237		Request to add Proposed solution should able to submit unknown files by its own to sandbox without user/administrator intervention and it should support up to 1,000,000 verdict queries per day. Remarks Automatic submission of unknown files to sandboxing without user intervention ensures real-time analysis and zero-delay protection against emerging threats. Supporting up to 1,000,000 verdict queries per day guarantees scalability for large environments, enabling high-volume threat detection without bottlenecks or performance degradation.	No change to prevent vendors locking in.
410	3.7.5 Server Security General Requirements 237		Request to add Proposed solution should have capability to search and destroy to swiftly sweep across endpoint and eradicate threats without any script Remarks Requiring a no-script search and destroy capability ensures even non-technical analysts can quickly locate and eliminate threats across all endpoints. This enhances operational efficiency, reduces response time, and	No change to prevent vendors locking in.

Enhancing Digital Government & Economy Project * BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			minimizes the risk of human error, enabling consistent and scalable threat remediation.	
411	3.7.5 Server Security General Requirements 237		Request to add Proposed solution must provide encryption management for BitLocker and file vault, it must be part of unified agent. Remarks Native encryption management for BitLocker and FileVault within a unified agent streamlines data protection and compliance without requiring additional tools. This simplifies policy enforcement, reduces agent sprawl, and ensures consistent visibility and control over endpoint encryption across the organization.	No change to prevent vendors locking in.
412	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution shall support high availability, redundancy, and scalability.	The proposed soluton must be able to achive high availability for indexing cluster without the need of any third party software and the solution should be DR ready and must support the data replication natively without relying on other third party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and	Please refer query response number 133

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			should be updated with artifacts for any incident analyst is working on. Remarks: To make it more use case driven and useful to BCC NSOC. As SIEM consists of multiple modules, writing on high availability, redundancy and scalability supports are not enough.	
413	Page 147, 3.7.1 Security Information and Event Management (SIEM) (4. General Requirement)	The proposed solution must be software-based allowing flexible deployment models and architecture.	The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per the requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters. Remarks: To ensure reliability and reduce TCO. As SIEM consists of multiple modules, mentioning the detail deployment model is more suitable and it will be easier to understand the proposed solution	Please refer query response number 134
414	Page 148, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or	The solution shall support parsing single-line and multi-line log files.	OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will	Please refer query response number 136

8

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	Ingestion Capabilities)		provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce TCO and make the solution reliable and always useful. Data parsers dependencies should be imposed to OEM for better efficiency	
415	Page 149, 3.7.1 Security Information and Event Management (SIEM) (5. Log Collection or Ingestion Capabilities)	The solution must support parsing, normalization or filtering of data before ingestion into the system.	The proposed solution must comes with apps and ad-ons for most common /well known security technologies and OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder. Remarks: To reduce the TCO and ensure availability of the parsers for any kind of data. Data parsers dependencies should be imposed to OEM for better efficiency	Please refer query response number 137
416	Page 149, 3.7.1 Security Information and Event Management (SIEM)	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per	Please refer query response number 138

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
	(5. Log Collection or Ingestion Capabilities)		new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time. Remarks: To make it more use case driven and useful to BCC NSOC, please change this clause as the change request	
417	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks The solution shall support multiple correlation methods like Vulnerability, Signature, Statistical, Historical, Heuristic and Predictive correlation. The solution shall have pre-built correlation rules for rapid deployment and coverage of common attack scenarios.	The proposed solution must come with at least 1200 out of the box correlation /detection rules to ensure and align with various industry security frameworks, allowing to readily monitor for potential threats across the systems and it should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.) The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques. Remarks: Request to change this as proposed. To ensure it covers all the attck scenarios and	Please refer query response number 139

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			reliable and updated to most lastest known and unknown attacks.	
418	Page 149, 3.7.1 Security Information and Event Management (SIEM) (6. Correlation & Detection Capabilities)	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user. Remarks: Request to change this as proposed. To ensure the solution is robust and reduce the overall false positives greatly scientifically.	Please refer query response number 140
419	Page 150, 3.7.1 Security Information and Event Management (SIEM) (7. AI/ML and UEBA Capabilities)	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	"The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. Proposed solution should use behavior modeling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect	Please refer query response number 141

Digital Government & Economy Enhancing Project ★
BCC
ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats. The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time. Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations. Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user. The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior. The proposed solution should have threat detection technique and models to distill anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together	

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			anomalies to provide an end-to-end story about a high-fidelity threat. Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields. The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors. The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI. The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain. The proposed solution should find deviations from typical behaviour or detection of interesting patterns like beaconing. The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity. The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.	

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time. Note: Bidder must comply with all the mandatory points in the technical and functional requirement as mentioned above, Non-compliance with any of the mandatory requirements may make the bid liable for rejection. Also, please understand that any of the above technical requirements mentioned needs to be demonstrated as asked during the evaluation phase. Remarks: Request to change this as proposed. To ensure a right solution that is useful to BCC NSOC is available and not just for the namesake, please add the technical use case driven specifications of UBA.	
420	Page 150, 3.7.1 Security Information and Event Management (SIEM) (8. Integration Feature)	The solution shall support integration with any SOAR platform.	The solution shall support integration with any third party solution with in-built plug ins and apps and platform and must have SOAR solution from same OEM to reduce any complexity.	Please refer query response number 142

Enhancing Digital Government & Economy Project
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Remarks: Request to change this as proposed. To ensure a end to end and seamless integration please rephrase	
421	Page 150, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution shall provide pre-built SOC dashboards and have compliance-ready reports (PCI DSS, ISO 27001, NIST, GDPR).	The solution shall provide pre-built SOC dashboards like Security Posture, Incident Review and Executive Summary dashboard to help ivestigate fatser and Top officials have the SOC visibility. - The solution shall have compliance-ready reports, solution which can be configured modified as per need by the auditter by bidder. Remarks: Request to change this as proposed. To make it effective and use case driven please rephrase.	Please refer query response number 143

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
422	Page 151, 3.7.1 Security Information and Event Management (SIEM) (9. Dashboard, Search & Reporting Capabilities)	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements. Remarks: Request to change this as proposed. To make sure it follows the standard process and less dependency and more coverage.	Please refer query response number 145

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
423	Page 152, 3.7.1 Security Information and Event Management (SIEM) (12. Licensing Option)	The supplier can offer any flexible and scalable licensing model based on the following baseline information: - Log Data Volume: 1500+ GB/day - EPS: 40,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value	Log Data Volume: 300+ GB/day - EPS: 8,000 or unlimited EPS - Retention: 30 days before archival - Redundancy factor: 1 - Unlimited log sources and EPS value Remarks: Requesting to please consider this proposed sizing. As all the CII will not be onboarded to the NSOC SIEM on day 1. So 1500 GB/day or 40,000 EPS are very high volume of data ingestion and will insure HUGE COST. As per our understanding, 300GB/day or 8,000 EPS should be sufficient for the operation. Kindly share the details of data sources for the right sizing of the solution for Day 1.	Please refer query response number 22
424	Page 152, 3.7.1 Security Information and Event Management (SIEM) (13. Compliance)	The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.	The offered solution shall be positioned either in the leader or Challengers quadrants for the last 5 consequtive years reports at Gartner Magic Quadrants for SIEM Remarks: Global Leaders for SIEM Solutions are listed in either Leaders or Challengers in the Gartner Magic Quadrant Reports. By adding Visionary will allow Startup solutions whose doesn't have much market references globally.	Please refer query response number 29

8

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
425	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (9. Integration)	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM	The offered solution shall have support to integrate with proposed SIEM or it can be an in-built solution of the SIEM Remarks: Request to change this as proposed. To ensure a end to end and seamless integration same OEM is cost effective	Please refer query response number 148
426	Page 154, 3.7.2 Security Orchestration, Automation, and Response (SOAR) (10. Licensing Option)	On-premise license for 50 analysts from day one and shall be scalable in the future.	0n premise license for 5 analysts from day one and shall be scalable in the future Remarks: Request to change this as proposed. 50 analysts licenses is too high for the NSOC requirement and insure HUGE COST. 5 analysts License should be enough considering 3 shifts operation as Licenses are concurrent in nature.	Please refer query response number 31
427	Page N/A, 3.7.9 Network Behavior Analysis (NBA) with Sandboxing	**(Not specified)**	Request to Add Proposed Solution should support data retention for minimum 30 Days Remarks: Log retention or data retention period is not mentioned. Requesting to include minimum 30 days of data retention	Please refer query response number 151
428	3.7.20 201-203		1. Room Size: Need Drawing or Floor Plan 2. Workstation: Will the table be up or down? 4. Small Meeting Agea: Module table design required. 8. Power Supply: Need full equipment power consumtion calculation.	Please request EDGE for the site survey. Based on that perform the site survey and get requirements.

Enhancing Digital Government & Economy Project ★ BCC ICT Division

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			14. Partitioning: How to use soundproofing in a small meeting room with a glass partition? 17. Speaker Setup: Need more information.	
429	VII 3.7.18 FC Storage 199	8. Minimum 300 TB usable space using NVMe SED drive without considering deduplication & compression after RAID 6	Minimum 300 TB usable space using NVMe SED drive without considering deduplication & compression after RAID 6 or dual/triple parity RAID; Remarks It will allow more OEM/Bidder for bidding	Refer to Addendum No.1 of RFP Document.
430	VII 3.7.18 FC Storage 200	19. System must have Hardware/Software based replication system with necessary licenses. Replication should be configured for data replication across metro and global distances for disaster recovery. Replication software should support synchronous as well as asynchronous replication. The system should support at least 3 site replications over IP and SAN.	System must have Hardware/Software based replication system with necessary licenses. Replication should be configured for data replication across metro and global distances for disaster recovery. Replication software should support synchronous as well as asynchronous replication. The system should support at least 3 site replications over IP or SAN. Remarks It will allow more OEM/Bidder for bidding	Refer to Addendum No.1 of RFP Document.
431	VII 3.7.16 197	SL. 7: Graphics: NVIDIA RTX 3080 or equivalent	Kindly specify the required graphics memory size (e.g., 2GB / 4GB / 8GB, etc.).	Refer to Addendum No.1 of RFP Document.

Enhancing Digital Government & Economy Project ★
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
432	VII 3.7.16 197	SL. 9: Monitor: Two side-by-side monitors (27" or 32"), one vertical monitor (24")	Please clarify the exact number of monitors required. Is it 2 or 3 units?	3 Units
433	VII 3.7.17 198	SL. 4: Processor: Intel Core i9 or equivalent	Currently, only the Ultra series processors are available. Kindly confirm the specific Ultra processor model required	The bidder will propose equivalent or higher product as per GCC.
434	VII 3.7.17 198	SL. 11: Keyboard and Mouse: Ergonomic Wireless Keyboard and Mouse	Wireless mouse is fine. However, the keyboard is built-in with the laptop. Do you require an additional wireless keyboard? Please clarify.	Yes
435	Section VII 3.7.20 SOC Room 201	Room Size: Space Utilization: 600 sqft. To utilize space effectively for 10-15 people, meeting rooms, and equipment.	"Room Size: Space Utilization: 600 sqft. To utilize space effectively for 10 people, meeting rooms, and equipment. Remarks "600 sq. ft. area is optimally suited for accommodating upto 10 people considering the inclusion of meeting rooms and other equipment setup. Ccordingly we request you to consider the proposed change. Please provide us with floor layout and measurements. "	No change.
436	Section VII 3.7.20 SOC Room 202	17. Speaker Setup : speaker per workstation. 15W speakers for each workstation or central speaker setup in the room for communication.	Speaker requirement should be specific, i.e. one speaker per workstation or one central speaker/s. Remarks:	The bidder will propose.

8

Enhancing Digital Government & Economy
BCC
ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
			Please specify any one option, and mention the required functionality.	
437	Section VII 3.7.20 SOC Room 202	18. Ambient Noise Level : Below 40dB. Minimized noise levels in the workspace for focus and clarity.	Floor layout and detailed existing wall, ceiling and floor matterial are needed for proper design. Remarks Please provide the required layout with measurements. Please arrange site visit asap basis.	Please request EDGE for the site survey. Based on that perform the site survey and get requirements.
438	Section VII 3.7.23 20 KVA online UPS (Qty. 01) 212	7. Output Voltage: 208 / 220 / 230 / 240 VAC + PE 2 Wires for 1 Phases (User Selectable) / ≤1%	220/230/240VAC (1-Phase), 380/400/415VAC (3-Phase) Remarks In our country 208 output voltage is of no use.	The bidder will propose which is suitable.
439	Section VII 3.7.23 20 KVA online UPS (Qty. 01) 212	13. Battery: Number of Battery: 12V 70 Ah x 16	12V 40Ah x 32 (our offered UPS required minimum 32 nos battery, so we are considering 40Ah battery instead of 70Ah; which is higher in battery capacity and will provide more backup time.) Remarks 32 x 40ah battery pack will provide longer backup time. Also maintenace will be easier	No change.

8

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
440	Section VII 3.7.24 Face & Fingerprint Time Attendance Access Control System 213	5. General Features: Powers supply by standard PoE and at the same time powers supply for door lock (12 VDC/1 A)	12 VDC, 1 A power adapter should be included for Access Control device and brackets Remarks As PoE-supported access control devices are not requal products and the required quantity is low, so we kindly request you to proceed with the proposed change.	No change.
441	Section VII 3.7.24 Face & Fingerprint Time Attendance Access Control System 214	9. PoE: IEEE802.3at, standard PoE	PoE: Not required Remarks As PoE-supported access control devices are not regular products and the required quantity is low, we request you to accept the proposed change for smooth maintenance and support.	No change.
442	VII 3.7.8 178	6. The proposed solution should be on-premise appliance or VM based deployment	The proposed solution should be built on modern container technologies deployable on containerized (like Docker, Kubernetes) mode. The solution should either support built-in Kubernetes technology or Bring Your Own Kubernetes (BYOK) platform provided by the bidder and the system must be FIPS 140-2 compliant, which ensures that cryptographic-based security system are to be used to provide protection for sensitive or valuable data.	No change.

Digital Government & Economy Enhancing Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
443	VII 3.7.8 178	8. The offered solution should be deployed in Windows and Linux platform	The offered solution should support deployment on latest version of Windows and Linux Operating System or combination of both with open-source database as backend and should be 64-bit application to fully utilize the server resources on which it is installed.	No change.
444	VII 3.7.8 178	10. Bidder must provide all necessary software for successful deployment of the offered solution without any extra cost	Bidder must provide all necessary software for successful deployment of the offered solution without any extra cost and proposed ITSM and NMS modules should be from Single OEM for a single pane of Glass view.	No change.
445	VII 3.7.8 178	12. User Portal Should be web based	The user Portal should be web nased and the proposed ITSM solution should be built on ITIL framework and must comply with at least 9 processes. The ITILv4 processes PeopleCert Gold certified that are relevant and need to be assessed to meet the minimum functional criteria are Incident Management, Problem Management, Change Enablement, Service Configuration Management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management, and Service Request Management. The certification copy to be submitted.	No change.
446	VII 3.7.8 179	43. Clone/Copy Ticket with unique ticket number & editable field of new ticket	Manual ticket creation with copy/paste of relevant info; unique ticket number auto-generated; all fields editable	Please refer query response number 63

Enhancing Digital Government & Economy Project ★ BCC ICT Division

	Page/ Clause Number/ Item Name	Page/Clause/ Requirement	Question/Clarification Sought	PE Response
447	VII 3.7.8 185	**200**. Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill- down capabilities**.**	should allow multiple network maps to be nested with drill- down capabilities.	No change.
448	VII 3.7.8 185	201. The proposed monitoring solution able to add interfaces as a component in a map to monitor the availability of interface/VLANs.	The proposed monitoring solution must be able to monitor the availability and performance of interfaces/VLANs per device, and provide visibility through status indicators, alerts, and drill-down dashboards. Visual representation on topology maps should include devices, with interface/VLAN-level metrics accessible through the device view	Please refer query response number 65

8

Enhancing Digital Government & Economy Project *
BCC
ICT Division