

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

Memo No: 56.01.0000.046.007.083.2025-163

Date: 06 August 2025

Project: Enhancing Digital Government and Economy (EDGE)

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

Request for Proposals (RFP) No: EDGE-G20

Addendum No. 1 to RFP No. EDGE-G20

This is for the information of all concerned Proposers that the following amendments have been made to Request for Proposals (RFP) No. EDGE-G20 "Supply, Installation and Commissioning of National Security Operation Centre (NSOC)" pursuant to ITP Clause 8 of the said RFP:

Sl. No.	RFP Reference	Issued RFP	As Amended
1.	Section II – Proposal Data Sheet (PDS) ITP 23.1 Page 50	For Proposal submission purposes only, the Purchaser's address is: Attention: Project Director, Enhancing Digital Government and Economy (EDGE) Project Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh The deadline for Proposal submission is: Date: 10 July 2025 Time: 12.00 hours Bangladesh Standard Time (BST= GMT + 6:00 hours)	For Proposal submission purposes only, the Purchaser's address is: Attention: Project Director, Enhancing Digital Government and Economy (EDGE) Project Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh The deadline for Proposal submission is: Date: 19 August 2025 Time: 12.00 hours Bangladesh Standard Time (BST= GMT + 6:00 hours)
2.	Section II – Proposal Data Sheet (PDS) ITP 26.1 Page 50	The Proposal opening shall take place at: Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh Date: 10 July 2025	The Proposal opening shall take place at: Address: Youth Tower (Level 5), 822/2, Rokeya Sarani, Dhaka-1216, Bangladesh Date: 19 August 2025



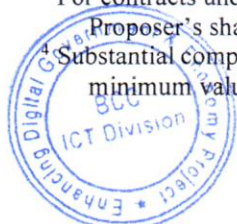
Sl. No.	RFP Reference	Issued RFP	As Amended
		Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).	Time: 12.30 hours Bangladesh Standard Time (BST= GMT + 6:00 hours).
3.	Section III – Evaluation and Qualification Criteria 1.3.2 Average Annual Turnover Page 67	Requirement Minimum average 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	Requirement Minimum average annual turnover of US\$ 3.5 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
4.	Section III – Evaluation and Qualification Criteria 1.4.2 Specific Experience Page 69-71	Requirement Participation as a prime supplier, management contractor, JV ¹ 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 ² 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	Requirement Participation as a prime supplier, management contractor, JV ³ 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 ⁴ 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

¹ For contracts under which the Proposer participated as a joint venture member or sub-contractor, only the Proposer's share, by value, and role and responsibilities shall be considered to meet this requirement.

² Substantial completion shall be based on 80% or more value completed under the contract and shall satisfy the minimum value of contract as required.

³ For contracts under which the Proposer participated as a joint venture member or sub-contractor, only the Proposer's share, by value, and role and responsibilities shall be considered to meet this requirement.

⁴ Substantial completion shall be based on 80% or more value completed under the contract and shall satisfy the minimum value of contract as required.



Sl. No.	RFP Reference	Issued RFP	As Amended
		<p>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).</p> <p>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).</p> <p>The successful supply completion certificate issued by the Proposer's parent/subsidiary/sister/affiliate firm will not be considered for specific experience.</p>	<p>contracts shall be documented by a copy of an Operational acceptance certificate (or equivalent documentation satisfactory to the Purchaser) issued by the purchaser(s).</p> <p>The successful supply completion certificate issued by the Proposer's parent/subsidiary/sister/affiliate firm will not be considered for specific experience.</p>
5.	<p>B. FUNCTIONAL, ARCHITECTURAL AND PERFORMANCE REQUIREMENTS</p> <p>1.2 Business Function Requirements to be met by the National Security Operation Center (NSOC)</p> <p>Page 135</p>	<p>1.2.1.3 Threat Intelligence Management</p> <ul style="list-style-type: none"> • 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. 	Text Dropped.
6.	<p>Section VII – Purchaser's Requirements</p> <p>3.7 Detailed Technical Specifications and Requirements</p>	<p>The proposed solution shall support high availability, redundancy, and scalability.</p>	<p>The bidders shall propose highly available, redundant and scalable design without any dependency on other platforms.</p>

8

12



Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7.1 Security Information and Event Management (SIEM) SL: 4 General Requirement Page 147		
7.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 4 General Requirement Page 147	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.
8.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 5 Log Collection or Ingestion Capabilities Page 148	The solution shall support parsing single-line and multi-line log files.	The solution shall support parsing single-line/multi-line log files.
9.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 5 Log Collection or Ingestion Capabilities Page 148	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.	The proposed solution must support the collection of logs and flows (NetFlow, sFlow, IPFIX) natively. Integration with a 3rd party Full Packet Capture solution is required only where applicable and should be supported by the proposed solution through standard integration mechanisms. Bidder must ensure compatibility and integration capability with industry-standard 3rd party packet capture solutions
10.	Section VII – Purchaser’s Requirements	The solution must support parsing, normalization or	The solution must support parsing, normalization or filtering of data before ingestion into the system. Moreover,



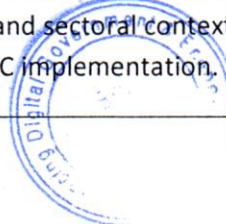
Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 5 Log Collection or Ingestion Capabilities Page 149	filtering of data before ingestion into the system.	the solution shall have built-in parsers widely popular and applicable for security analysis.
11.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 5 Log Collection or Ingestion Capabilities Page 149	The solution must support parsing of old data with new parser without re-ingesting or re-indexing.	The solution must support parsing and viewing of historical data using updated parsers or schemas without requiring data to be re-ingested, re-indexed, or stored redundantly. The system should allow retrospective analysis of previously ingested data in new formats to support use cases such as predictive analytics, proactive threat monitoring, and incident forensics, thereby optimizing storage and operational efficiency.
12.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 6 Correlation & Detection Capabilities Page 149	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 shall support time-series correlation across long-term event data to detect multi-stage, slow-moving, or hidden attacks, and shall support multiple correlation methods including Vulnerability, Signature, Statistical, Historical, Heuristic, and Predictive correlation. The solution must come with necessary correlation and detection rules out-of-the-box which are aligned with industry-standard frameworks such as MITRE ATT&CK, CIS, NIST, and the Cyber Kill Chain and provide intuitive dashboard to drill down for analysis.
13.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM)	The solution shall support real-time threat detection, with risk-based alert prioritization.	The solution shall support real-time threat detection, with risk-based alert prioritization. The risk based approach shall ensure prioritizing critical incidents, reducing false positives, and support effective incident response through risk-driven triaging.

Sl. No.	RFP Reference	Issued RFP	As Amended
	SL: 6 Correlation & Detection Capabilities Page 149		
14.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 7 AI/ML and UEBA Capabilities Page 150	The solution shall include built-in UEBA capabilities to establish baseline behavior patterns for users, entities, and devices, and detect deviations (anomalous activities).	The proposed solution shall include a built-in UEBA module capable of establishing heuristic and multidimensional baselines of user, entity, and device behaviors using unsupervised machine learning, statistical modeling, and peer-group analysis. It shall detect anomalies by continuously analyzing deviations from established patterns and combining these into actionable threat narratives including identity resolution of different entities. The UEBA module must detect complex threats such as lateral movement, data exfiltration, and beaconing through graph-based analytics that aggregate related anomalies. It shall provide real-time threat investigation capabilities to analysts from intuitive dashboard.
15.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 8 Integration Feature Page 150	The solution shall support integration with any SOAR platform.	The proposed SIEM solution shall support integration with any third-party SOAR platform through standard APIs, built-in connectors, apps, or plugins. Additionally, to reduce implementation complexity and ensure streamlined operations, the solution should provide pre-built integration templates and centralized orchestration capabilities for common SOAR platforms.
16.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL: 11	The proposed SIEM solution shall meet the standard (PCI DSS, ISO 27001, NIST CSF etc.) and out-of-box compliance.	The proposed SIEM solution shall support compliance with internationally recognized standards and frameworks (e.g., PCI DSS, ISO/IEC 27001, 27017, 27018, NIST CSF, SOC 2, GDPR), with out-of-the-box capabilities where applicable to the regulatory and sectoral context of a national SOC implementation.



8

[Handwritten signature]



Sl. No.	RFP Reference	Issued RFP	As Amended
	(Security and Compliance) Page 151		
17.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.1 Security Information and Event Management (SIEM) SL:11 Security and Compliance Page 152	The solution must have MITRE ATT&CK Rule Mappings.	The proposed solution must include MITRE ATT&CK rule mappings and provide comprehensive detection use cases with guidance on assessing security threats and investigating them using the platform.
18.	Section: 3.7 Detailed Technical Specifications and Requirements, 3.7.1 Security Information and Event Management (SIEM), SL: 12 Licensing Option Page: 152	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	The licensing model must be scalable in future. The implementation will be done in way that license requirements will grow over time. Year 1 - - Estimated Log Data Volume: Minimum 700 GB/day - EPS: Minimum 20,000 EPS (with Queuing Support) - Retention: Minimum 30 days before archival - Redundancy Factor: 1 - Support for unlimited log sources - Onboarding of at least 5 CIIs as per NSOC's guidelines. Year 2 - - Estimated Log Data Volume: Minimum 1050 GB/day - EPS: Minimum 30,000 EPS (with Queuing Support) - Retention: Minimum 30 days before archival - Redundancy Factor: 1 - Support for unlimited log sources - Onboarding of more CIIs as per NSOC's guidelines. Year 3 - - Estimated Log Data Volume: Minimum 1750 GB/day



Sl. No.	RFP Reference	Issued RFP	As Amended
			<p>- EPS: Minimum 40,000 EPS (with Queuing Support)</p> <p>- Retention: Minimum 30 days before archival</p> <p>- Redundancy Factor: 1</p> <p>- Support for unlimited log sources</p> <p>- Onboarding of more CII's as per NSOC's guidelines.</p> <p>After 3 Years Post Warranty:</p> <p>"Based on Business requirement & capacity of CII, it will be increase following NSOC procurement plan."</p> <p>Additional Note: The supplier must propose a tiered, consumption-based, or modular licensing model that avoids upfront overprovisioning and enables cost-effective scaling.</p> <p>Flexibility is required to adjust based on actual onboarding rates and entity-specific data volume patterns.</p> <p>Licensing cost breakdown per year/tier must be included in the financial proposal.</p>
19.	<p>Section:</p> <p>3.7 Detailed Technical Specifications and Requirements,</p> <p>3.7.1 Security Information and Event Management (SIEM)</p> <p>SL 13.</p> <p>Compliance</p> <p>Page: 152</p>	<p>The offered solution shall be positioned either in the leader or visionaries quadrant of latest Gartner Magic Quadrants for SIEM published in 2024</p>	<p>The offered solution shall be positioned in the in the Leaders, Visionaries, or Challengers quadrant of latest Gartner Magic Quadrants for SIEM published in 2024.</p>

8

✓



Sl. No.	RFP Reference	Issued RFP	As Amended
20.	<p>Section VII – Purchaser’s Requirements</p> <p>3.7 Detailed Technical Specifications and Requirements</p> <p>3.7.1 Security Information and Event Management (SIEM)</p> <p>SL: 16</p> <p>Preferred: Gartner Magic Quadrant-Based Product Evaluation</p> <p>Page 152</p>	<p>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.</p>	<p>Proposer will be awarded 2 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category in 2024. Products ranked as a Leader in 2024 will score 4. Products ranked as a Visionary in 2024 will score 3, Products ranked as a Challenger in 2024 will score 2. No points will be awarded if no valid Gartner documentation is provided. The proposer must submit verifiable Gartner Magic Quadrant reports or excerpts for 2024 to support their claims.</p>
21.	<p>Section VII – Purchaser’s Requirements</p> <p>3.7 Detailed Technical Specifications and Requirements</p> <p>3.7.2 Security Orchestration, Automation, and Response (SOAR)</p> <p>SL: 10</p> <p>(Licensing Option)</p> <p>Page 154</p>	<p>On premise license for 50 analysts from day and shall be scalable in the future</p>	<p>The supplier shall provide an on-premise license for 50 analysts from day one, with the capability to scale as needed in the future. However, the licensing model must align with industry-standard SOC practices where license consumption applies only to users with administrative privileges. The proposed licensing structure must meet the following conditions:</p> <p>License consumption must be limited to Admin Users responsible for:</p> <ul style="list-style-type: none"> Access control Feature allocation Compliance and auditing <p>For non-admin roles such as:</p> <ul style="list-style-type: none"> Threat hunting Incident response Read-only viewers <p>The solution must remain scalable to allow the addition of Admin users as</p>



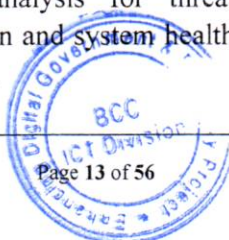
Sl. No.	RFP Reference	Issued RFP	As Amended
			operational demands grow. This licensing approach is expected to support efficient and cost-effective implementation while remaining compliant with the operational model of a large-scale National SOC.
22.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.3 Privileged Access Management (PAM) SL: 6 General Features Page 161	Solution must be from leaders quadrant of Gartner report for PAM.	The offered solution shall be positioned in the in the Leaders, Visionaries, or Challengers quadrant of latest Gartner Magic Quadrants for PAM published in 2024.
23.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.3 Privileged Access Management (PAM) SL: 12 Access and Session Management Page 161	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.	The solution should have login security by limiting user login based on enforceable parameters such as originating IP address, geographical location, and time of day. It should also support limiting concurrent login sessions per user.
24.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.3 Privileged Access Management (PAM) SL: 13 Remote Users Management Page 161	Solution must have biometric and password less authentication feature for remote users	Solution must have authentication feature for users With 2FA authentication.
25.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR)	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	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

Sl. No.	RFP Reference	Issued RFP	As Amended
	SL: 4 Brief Description Page 163	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.	changes, process executions, memory operations, and network connections. The EDR should utilize various detection techniques including behavioral analysis, AI/ML-based signatureless detection, 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.
26.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 5 Agent Deployment Page 163	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 actively supported operating systems. The supported platforms must include: Latest Version of Windows: 10, 11, Server 2012, 2016 (Extended Support), 2019 (Extended Support), 2022 macOS: 10.13 and above Server Security Solution in the RFP must support Linux (major distributions including RHEL, Debian, Rocky, Ubuntu, CentOS, SUSE).
27.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.3 Privileged Access Management (PAM) SL: 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	Proposer will be awarded 2 to 4 based on the positioning of their proposed product in the Gartner Magic Quadrant for the relevant category in 2024. Products ranked as a Leader in 2024 will score 4. Products ranked as a Visionary in 2024 will score 3, Products ranked as a Challenger in 2024 will score 2. No points will be awarded if no valid Gartner documentation is provided. The proposer must submit verifiable Gartner Magic Quadrant

Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 163	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.	reports or excerpts for 2024 to support their claims.
28.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 9 Threat Intelligence Integration Page 165	The EDR should integrate with TAXII/STIX feeds for automated intelligence updates.	Text to Added The EDR should integrate with threat intelligence feeds for automated intelligence updates. Note: Bidder can propose integration with TAXII/STIX and/or other industry-standard threat intelligence formats, provided the solution can ingest automated, real-time threat data to improve detection and response capabilities.
29.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 10 False Positive Management Page 165	The solution should provide tools for exception management with approval workflows.	The solution should provide tools for exception management with approval workflows from service desk.
30.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 11 Response and Remediation Capabilities	The solution must provide configurable automated response actions including process termination, file quarantine, network isolation, and user session termination.	The solution must provide configurable automated response actions including process termination, file quarantine, network isolation. Capability for user session termination is desirable, where supported.



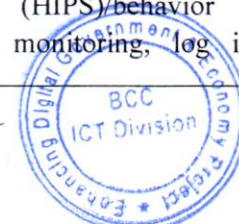
Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 165		
31.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 11 Response and Remediation Capabilities Page 165-166	The EDR should support the creation of custom 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.	Text Removed.
32.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 11 Response and Remediation Capabilities Page 166	The solution must support live response capabilities with minimal latency (<5 seconds).	The solution must support live response capabilities with minimal latency, preferably within 5 seconds under normal operating conditions.
33.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 11 Response and Remediation Capabilities Page 166	The solution must enable system remediation actions including forced logoff, restart, or shutdown.	The solution must enable system remediation actions including forced logoff, restart, or shutdown, as well as actions such as Terminate process, Delete file, Clean persistent data, and Block address on Firewall.
34.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements	The EDR should include trend analysis for threat detection and system health metrics.	Text Removed



Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7.4 Endpoint Detection and Response (EDR) SL: 12 Management and Administration Page 167	The EDR should include a query language for custom data analysis and reporting.	
35.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 14 Data Management and Compliance Page 168	The EDR should include features for compliance with HIPAA, PCI DSS, and other relevant regulations.	The EDR should include features or integrated with other tool for compliance e. g HIPAA, PCI DSS, and other relevant regulations and compliance with industry standard.
36.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 17 User Behavior Analytics Page 169	The solution should establish user behavior baselines for anomaly detection.	The solution should establish user behavior baselines for anomaly detection, including but not limited to malware-related activities.
37.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 17 User Behavior Analytics Page 169	The EDR must detect suspicious user activities that may indicate account compromise.	Amendment: The EDR must detect suspicious user and malware activities that may indicate account compromise
38.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.5 Server Security SL: 10 General Requirements	The proposed server security solution has Antimalware, Application & device control, Web reputation, Host based firewall Host-based intrusion prevention	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 inspection

8

✓

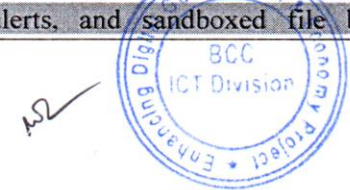


Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 170	solution (HIPS)/behavior analysis, Integrity monitoring, log inspection module along with sandbox integration in the same single agent.	module along with sandbox integration in the same single agent
39.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.5 Server Security SL: 10 (General requirement) Page 170	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 on premises solution but will protect all type of server (physical, virtual, cloud) from a single console. For Product Security, Patch, Signature can be communicated with Cloud.
40.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.6 Next Generation Firewall for SOC (Qty. 02) SL: 11 Next Generation Firewall Security Features Page 172	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.	The firewall should provide latest & rich URL category database with minimum 240 million URLs and accelerates access to specific categories of websites, improving access experience of high priority websites.
41.	Section VII – Purchaser's Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.7 VPN Firewall for CII Integration SL: 11 Next Generation Firewall Security Features Page 176	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.	The firewall should provide latest & rich URL category database with minimum 240 million URLs and accelerates access to specific categories of websites, improving access experience of high priority websites.
42.	Section: 3.7 Detailed Technical Specifications and Requirements,	NMS Module	Title changed as: NMS Module A



Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7.8 Ticketing, IT Service, IT Asset & NMS System SL: 141-213 Page:182		
43.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.8 Ticketing, IT Service, IT Asset & NMS System SL: 200 Display Page 185	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drilldown capabilities.	Background and icon customization is desirable but not mandatory, should be support multiple network maps with nesting and drill-down capabilities is essential and must be fulfilled by the proposed solution. Bidder has to be clearly specified the extent of available customization features in their technical proposal.
44.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.8 Ticketing, IT Service, IT Asset & NMS System SL: 201 Display Page 185	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. Visual representation on topology maps should include devices, with interface/VLAN level metrics accessible through the device view
45.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.9 Network Behavior Analysis (NBA) with Sandboxing SL: 7 Sandbox Environment Page 187	The solution shall ensure process, registry, file system, network connection, and memory manipulation monitoring with API call analysis.	Following Text Removed. The solution shall ensure process, registry, file system, network connection, and memory manipulation monitoring with API call analysis.
46.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements	Null	Feature added in the Serial Number 9. The Network Behavior Analysis (NBA) solution with sandboxing must support a minimum data retention period of 30 days for all relevant logs, metadata, alerts, and sandboxed file behavior

8



Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7.9 Network Behavior Analysis (NBA) with Sandboxing SL: 9 Management and Reporting Page 187		outcomes. The solution should also allow configurable retention policies to meet operational and compliance requirements according to industry standards and best practices.
47.	Section: 3.7 Detailed Technical Specifications and Requirements, 3.7.13 Access Switch for SOC Room and Management 15 Management Page: 193	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow	SSHv2, Telnet, SNMPv3, Syslog, AAA, RADIUS, RMON, sFlow/Netflow. Bidder are allowed to propose equivalent or higher as per industry standard protocol compliance.
48.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.16 Workstation SL: 7 Graphics Page 197	Graphics: NVIDIA RTX 3080 or equivalent	Graphics: NVIDIA RTX 3080 or equivalent with memory size minimum 8GB.
49.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.18 FC Storage SL: 8 Capacity Requirements Page 199	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
50.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.18 FC Storage SL: 19 Replication Page 200	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	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.



Sl. No.	RFP Reference	Issued RFP	As Amended
		site replications over IP and SAN.	
51.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.22 Video wall system SL: 1 Pixel Pitch Page 205	min 0.5 mm	Minimum pixel pitch of 0.5 mm or 0.63 mm (H) × 0.63 mm (V), complying with standards for video walls.
52.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.22 Video wall system SL: 1 Physical Seam Page 205	Min. 0.6 mm	Minimum pixel pitch of 0.6 mm and pixel pitch up to 0.88 mm will also be considered.
53.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.22 Video wall system SL: 1 Resolution Page 205	at least 4K (3840x2160)	at least 1920×1080 (FHD)
54.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.22 Video wall system SL: 1 Casing Material Page 205	SGCC	SGCC or equivalent high-quality metal material which is suitable for video wall durability and structural requirements.
55.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.22 Video wall system SL: 1 Brightness	700 cd/m ² minimum	500 cd/m ² minimum

8

me



Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 205		
56.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.24 Face & Fingerprint Time Attendance Access Control System SL: 8 Wi-Fi Page 214	Wi-Fi must support dual-band (2.4 GHz and 5 GHz) for better stability	Wi-Fi must support dual-band (2.4 GHz or 5 GHz) for better stability.
57.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.27 External Attack Surface Management SL: 9 Dashboard and Reporting Page 220	The solution shall have feature to create template for custom report generation	The solution shall have features to create templates for custom report generation, including the ability to filter reports by date range, keywords, categories, and relevance to security threats.
58.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.28 Malware Analysis Sandbox (On-premise) SL: 7 Analysis Capabilities Page 222	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, and activated copies of operating systems and applications (e.g., Microsoft Office) as applicable, with no requirement for the customer to purchase additional licenses separately. All necessary licenses must be quoted by the bidder to ensure the system is fully functional from day one. Furthermore, the licensing model should support unlimited sample analysis with no named user restrictions. If there are any concurrency limits, they must be clearly defined in the proposal to enable proper evaluation of the solution’s scalability and cost-effectiveness.
59.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements	The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through inbuilt MITM proxy.	The solution should provide capabilities for analyzing encrypted SSL/TLS traffic artifacts through an inbuilt MITM proxy or integration with

Sl. No.	RFP Reference	Issued RFP	As Amended
	3.7.28 Malware Analysis Sandbox (On-premise) SL: 8 File and Protocol Support Page 223		network security devices that perform SSL/TLS inspection.
60.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.28 Malware Analysis Sandbox (On-premise) SL: 9 Integration and Reporting Page 223	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, leveraging network data and/or threat intelligence sources where possible.
61.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.28 Malware Analysis Sandbox (On-premise) SL: 10 Compliance and Data Protection Page 224	The solution OEM must have appropriate or attestations for relevant data protection laws (e.g., ISO 27001, SOC 2 Type II, GDPR etc.).	The proposed Malware Analysis Sandbox solution shall meet the standard (e.g PCI DSS, ISO 27001, 27017, 27018, NIST CSF, HIPPA, SOC 1, SOC 2, SOC3, etc.) and out-of-box compliance.
62.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.28 Malware Analysis Sandbox (On-premise) SL: 13 Preferred: Malware Analysis Sandbox Page 224	Ability to host the solution in one or more hypervisor	The solution should support deployment on one or more hypervisors (e.g., VMware, Hyper-V, KVM) and/or other deployment formats such as physical appliances or cloud-based environments.
63.	Section VII – Purchaser’s Requirements 3.7.32 Project Management Oversight (Non-Priced) for NSOC System Implementation	SOC project management organization	New text added. The Bidder should be, or be supported by, a globally experienced and skilled technology company with demonstrated expertise in the design,

Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 227		management, and implementation of National Level SOC's internationally.
64.	3.7 Detailed Technical Specifications and Requirements	<p>3.7.29 SOC Trainings (With Certification Exams)</p> <p>3.7.30 SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)</p> <p>3.7.31 Installation & Implementation of NSOC System</p> <p>3.7.32 Project Management Oversight (Non-Priced) for NSOC System Implementation</p> <p>3.7.33 Service Level Agreement (SLA)</p> <p>3.7.33.1 Operational and Maintenance Personnel during SLA</p>	<p>Serial Number Changed as:</p> <p>3.7.31 SOC Trainings (With Certification Exams)</p> <p>3.7.32 SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)</p> <p>3.7.33 Installation & Implementation of NSOC System</p> <p>3.7.34 Project Management Oversight (Non-Priced) for NSOC System Implementation</p> <p>3.7.35 Service Level Agreement (SLA)</p> <p>3.7.35.1 Operational and Maintenance Personnel during SLA</p>
65.	<p>Section VII – Purchaser's Requirements</p> <p>3.7 Detailed Technical Specifications and Requirements</p> <p>3.7.4 Endpoint Detection and Response (EDR)</p> <p>SL: 8</p> <p>Detection Capabilities</p> <p>Page 146</p>	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 signature-based/Signatureless, behavioral analysis, machine learning, and IOC matching.
66.	<p>Section VII – Purchaser's Requirements</p> <p>3.7 Detailed Technical Specifications and Requirements</p> <p>3.7.4 Endpoint Detection and Response (EDR)</p> <p>SL: 11</p> <p>Response and Remediation Capabilities</p>	The EDR should provide tools for credential reset or revocation when compromise is detected.	<p>Following Text Removed</p> <p>"The EDR should provide tools for credential reset or revocation when compromise is detected."</p>



Sl. No.	RFP Reference	Issued RFP	As Amended
	Page 165		
67.	Section VII – Purchaser’s Requirements 3.7 Detailed Technical Specifications and Requirements 3.7.4 Endpoint Detection and Response (EDR) SL: 17 User Behavior Analytics Page 169	The solution should correlate user activities across multiple endpoints to identify patterns.	Following Text Updated replace the previous one: The solution should correlate user and malicious activities across multiple endpoints to identify patterns.

8

mp



Sl. No. 68.

Section VII – Purchaser's Requirements

3.7 Detailed Technical Specifications and Requirements,

3.7.1 Security Information and Event Management (SIEM)

Page: 152

As Amended: for SIEM Probe/Sensor

Following Requirements added after SIEM Sl.16 Preferred Page 152 of RFP Document:

Sl.	Feature	Requirement of Procuring Entity
17	Solution Type: SIEM Probe/Sensor	The solution should be on premise and should not require internet access for day-to-day functionality. Any required update should be supported offline.
18	Brand/Product Name	To be mentioned by the bidder
19	Country of Origin	To be mentioned by the bidder
20	Quantity	10 Units (5 Pairs)
21	General Requirement	<p>The solution should support continuous full packet capture at all sites, for intended traffic (not just malicious traffic) to enable forensic investigations and threat hunting without the need for any 3rd party solution integrations and VM/host. Packet access and queries should not be limited to just the last few hours but provide access to all stored packets.</p> <p>The solution should natively support analyzing raw network packet data, including UDP traffic, from layer 2 to layer 7 of the OSI stack for complete threat analysis. The solution should not be limited to only sampled or meta-data (e.g., IPFIX or Net Flow) analysis. The analysis should be performed within the platform without requiring PCAP download.</p> <p>The solution should provide an independent and comprehensive analysis of the attack surface by uniquely identifying and profiling endpoints (servers, endpoints, IOT devices, virtual machines, etc.) based on behavioral fingerprints without depending on endpoint agent-based solutions or required integrations, simple DNS lookups etc.</p> <p>The solution should support profiling and tracking endpoints (managed and unmanaged) irrespective of IP address changes, location change, lack of MAC address visibility and / or login credentials change, without any external information sources.</p> <p>The solution should have capabilities to identify historical information about all endpoints (including unmanaged and IOT, if</p>

Sl.	Feature	Requirement of Procuring Entity
		<p>any) where the user has logged in without the need to integrate with any other solutions. The solution should support search for user or device names.</p> <p>The solution should be able to natively identify the fingerprints from network traffic including but not limited to domains, ciphersuites exchanged in TLS handshake, HTTP body hash etc. and should be capable to support all the following features without exception:</p> <ul style="list-style-type: none"> • Provide commonality & frequency analysis for each such fingerprint. • Provide a mechanism to search 90-days historical data for fingerprints without additional storage requirements. • Distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) • Track back to the actual traffic matching the fingerprint. • Automatically group similar devices together for forensic and outlier analysis. • Group devices based on a combination of fingerprints, provide an explanation of the similarity, and identify packet captures corresponding to that fingerprint. <p>The solution should be able to identify malicious activity by tracking commonality & frequency without requiring a baseline, threat intelligence or training period.</p> <p>The solution should support and provide examples at a minimum, all the following data science methods:</p> <ul style="list-style-type: none"> • Supervised machine learning • Unsupervised machine learning • Deep neural networks • Belief propagation • Multi-dimensional clustering • Decision tree classification • Outlier detection <p>The solution should out of the box provide details on domains accessed from the environment including date of first and last access, WHOIS information, subdomains accessed, protocols used, and bytes transferred, per device. The domain should have a risk score, and domain category listed.</p> <p>The solution should maintain an updated 90-day profile of all endpoints including a summary of protocol history to aid in the discovery of low-and-slow attacks.</p>

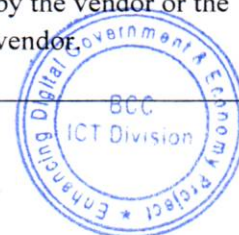
8



Sl.	Feature	Requirement of Procuring Entity
		<p>The solution should detect threats in encrypted traffic without the need to decrypt. For example, the solution should check the commonality and frequency of TLS ciphers and destinations, without requiring support from existing network switches, endpoint agents, network proxies or threat intelligence feeds. The solution should not limit itself to comparing JA3 hash values or reporting weak ciphers.</p> <p>The solution should have search capabilities that allow the end user to search over a minimum of 90 days of traffic history for any or all of the following: IP addresses, domain, username, email addresses or device names. All advanced analytics capabilities should be supported for all devices with the ability to query a minimum of 90 days of history without requiring 3rd party integrations.</p> <p>The solution should have an advanced search feature that allows the end user to search for any metadata field value combination including:</p> <ul style="list-style-type: none"> • Mac Address • TLS Cipher suite • TLS Server Name • TLS certificate fields • Web browser version • JA3 value • Various protocol headers <p>The solution should not depend exclusively on static rules such as IDS signatures, Suricata, Yara rules, baselines/thresholds or threat intelligence feeds for threat detection. The solution instead should primarily use artificial intelligence-based approaches to detect attacks.</p> <p>The solution should detect and respond to threats based on MITRE ATT&CK tactics and techniques and report the appropriate MITRE ATT&CK tactic and /or technique in the platform user interface.</p> <p>The solution should detect threats within clients such as VDI instances and containers even if these do not have any logging or endpoint security deployed within and without relying on IOCs and IDS signatures.</p> <p>The solution should support identifying and analyzing all devices without the need for endpoint agent installation, integration or simply DNS lookups.</p> <p>The solution should detect data exfiltration via methods including but not limited to DNS or ICMP tunnelling.</p>



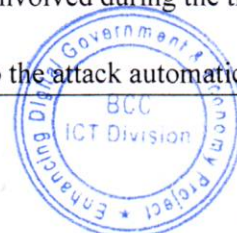
Sl.	Feature	Requirement of Procuring Entity
		<p>The solution should out of the box detect command and control to web domains that are rare in the customer environment without relying on indicators of compromise (IOC), IDS signatures, web reputation systems or threat intelligence.</p> <p>The solution should detect malicious browser extensions (man-in-the-browser attacks) that can be used to steal sensitive and private data without the need for any endpoint agent or integration with any other solutions, to provide an independent threat assessment.</p> <p>The solution should out of the box detect the use of defense evasion techniques such as proxy usage to hide data exfiltration and user agent spoofing to hide the source application without relying on indicators of compromise (IOC), IDS signatures, web reputation systems or threat intelligence.</p> <p>The solution should detect when attack tools are shared over SMB (file share) via protocol analysis (e.g. DCERPC) and without requiring access to Windows logs or other data sources.</p> <p>The solution detect indicators of compromise and early warning signs of ransomware such as the use of doppelganger domains, inbound remote desktop, clear text passwords, unauthorized use of remote management tools, etc.</p> <p>The solution should detect living-off-the-land attacks that use tools such as PSEXEC, PowerShell, WMI, remote registry etc using network data and without depending on the threat intelligence.</p> <p>The solution should detect use of remote management tools from non-admin devices without the need for manual tagging of devices.</p> <p>The solution should fully expose the definitions for all out of the box vendor provided threat detection techniques (models) and allow for their easy modification or adaptation. Detections should not be limited to Suricata, Zeek or other IDS alerts.</p> <p>The solution should support a fully transparent and extensible language for building custom threat detections based on a minimum of 1000 network attributes including but not limited to protocol information, device information, domain information, threat intelligence etc.</p> <p>The solution should also provide a minimum of 300 out of the box, reusable building blocks that can be used for custom threat hunting. All detection models (whether provided by the vendor or the community) should be supported by the vendor.</p>



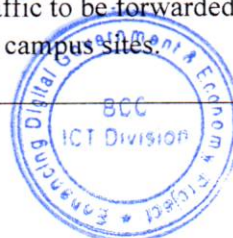
Sl.	Feature	Requirement of Procuring Entity
		<p>The solution should support automated and manual threat hunting, triage & investigations by surfacing the appropriate information needed by the security team. The solution should also allow the security team to add additional context and information to automated threat reports.</p> <p>The solution deployed in both online and offline modes should support analysis of network encrypted traffic without the need to decrypt and without the need for any endpoint agents or additional solutions.</p> <p>The solution should natively support extraction of a single PCAP based on a device, particular network activity, threat etc. irrespective if the device has changed IP addresses, time elapsed etc. This capability should be exposed both through the user interface and an API.</p> <p>The solution should detect the use of unencrypted credentials on the network, passwords stored in unencrypted formats as well as the use of insecure protocols without the need for any endpoint agent or integration with any other solutions, to provide an independent threat assessment.</p> <p>The solution should support tagging and annotation of 1 or more critical devices with a single operation. The solution should also support the use of these tags for the purpose of building custom threat detection or compliance models.</p> <p>The solution should detect Kerberos brute force attacks and capture the client name, server name, and error message for all Kerberos requests (not just attacks) and store these details for at least 90 days in a searchable format.</p> <p>The solution should detect DNS tunnelling attempts and allows the end user to easily change the detection parameters based on record type (MX, TXT, CNAME, A), DNS recursion, TTL and other criteria.</p> <p>The solution should monitor, track and extract field: value from all LLMNR traffic, including:</p> <ul style="list-style-type: none"> • LLMNR Request Question Name • LLMNR Response Answer Name • LLMNR Response Question Name • LLMNR Response Answer TTL <p>The solution should monitor, track and extract field: value from all SMB traffic, including:</p>



Sl.	Feature	Requirement of Procuring Entity
		<p>Kerberos Principal</p> <ul style="list-style-type: none"> • Kerberos Realm • NTLM Domain • NTLM Server Domain Name • NTLM Target Name • NTLM Username • File Actions • File ID • File Name • SMB Version • SMB Type • Share Type <p>The solution should monitor, track and extract field: value from all DCERPC traffic:</p> <ul style="list-style-type: none"> • DCERPC Bind Accepted UUIDs • DCERPC Bind Accepted UUIDs • DCERPC Bind UUID • DCERPC Bind Interface Major Version • DCERPC Bind Interface Minor Version <p>The solution should identify ransomware, executables, and other file types that are transferred via SMB file shares by parsing the SMB protocol. The solution should be able to create a custom file share detection model based on end user file names (SMB honeypot).</p> <p>The solution should detect DCERPC enumeration techniques, such as: services enumeration, computer name enumeration, domain groups enumeration, password policy enumeration, and remote file process execution.</p> <p>The solution should support all the following features without exception, under incident management workflow component with built-in automation that automatically:</p> <ul style="list-style-type: none"> • Visually maps out the devices and external destinations involved in the incident • Visually maps the relationships between the devices involved using machine learning and not solely based on simply correlating all connections to a known malicious IP or domain. • Use natural language processing and topic modelling to ingest and add context to the incident based on open source and threat intelligence sources, including if permitted by looking up the Internet. anonymously (without disclosing the organization's identity). • Provides complete audit of the automated investigation. • Mark legitimate activities of the devices involved during the time of incident • Suppress activities that are not relevant to the attack automatically.



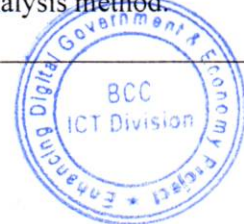
Sl.	Feature	Requirement of Procuring Entity
		<ul style="list-style-type: none"> Automatically generates an incident of the attack when new traffic is added. Provides a PDF report that can be independently shared outside the solution. <p>The solution should support customizable dashboards that can be:</p> <ul style="list-style-type: none"> Assigned to individual users Emailed on a scheduled basis Exported as a PDF to share outside the system <p>The solution should support retrospective detection and hunting for threats for a lookback period of up to 90 days, even if the traffic was assumed to be benign in the past.</p> <p>The solution should be able to classify and display applications and protocols across multiple protocol families including at a minimum:</p> <p>Application Family-Description</p> <ul style="list-style-type: none"> Antivirus-Antivirus update Compression-Compression layers Encrypted-Encryption protocol ERP-Enterprise Resource Planning application Forum-Web forum Mail-Email exchange protocol Middleware-Platform protocol for remote procedure calls Terminal-Remote terminal protocol Wap-Mobile specific transport protocol Web-Generic web traffic Webmail-Web email application
22	Integration capabilities	<p>The solution should support a RESTful API and syslog forwarding to push alerts to ticketing systems and other 3rd party systems to assist workflow management.</p> <p>The solution should support out-of-the-box integrations with at least 2 leading SIEM solutions from different OEMs.</p> <p>The solution should support out-of-the-box integrations with at least 2 leading EDR solutions from different OEMs.</p> <p>The solution should provide a RESTful API to allow endpoint detection & response (EDR) and security orchestration (SOAR) to implement response actions.</p> <p>The solution should provide a RESTful API to support packet capture (PCAP) export.</p>
23	Deployment Requirement	<p>The solution should support a scale-out, distributed architecture that does not require all raw traffic to be forwarded to a central analytics engine(s) from the various campus sites.</p>



Sl.	Feature	Requirement of Procuring Entity
		<p>The solution should store all packet captures at the collection site and only forward minimal metadata to the analytics engine(s).</p> <p>The solution should provide full functionality based solely on the capture and analysis of raw traffic, without requiring other inputs such as NetFlow/Sflow, logs, APIs, endpoint agents or other integrations, to get an independent security view of the infrastructure during outages or attacks.</p> <p>The solution should support a single user interface across geographically dispersed analytics engines deployments.</p> <p>All licensing should be quoted along with the product required for the specification asked. Any new software upgrades, features and threat detection models that come out in the future and should be available at no additional cost for the duration of the contract.</p> <p>All required licenses for 3rd party integration should be included in the solution from day 1. Any integration that may be required in future should not be of any additional cost, for the duration of the contract.</p> <p>The solution should not require visibility into MAC addresses of devices to simplify sensor deployments.</p> <p>The solution should support cold standby nuclei for high availability of the metadata without any Packet broker solutions.</p> <p>The solution should detect Non browser HTTP and TLS sessions without the need for any endpoint agent or integration with any other solutions, to provide an independent threat assessment.</p> <p>The solution should detect HTTP BasicAuth content-encoding method and should be able to search historical data for the encoded string.</p> <p>The solution should detect Golden Ticket attack without any integrations, context from another solution.</p> <p>The solution should detect the exploitation of Zero Logon vulnerability without profiling information from any other sources.</p> <p>The solution should profile the devices without any endpoint agent or original Mac address or any other solution components and should be able to identify the uncommon activities for the profiled devices through the commonality & frequency analysis method.</p>

8

2



Sl.	Feature	Requirement of Procuring Entity
		<p>The solution should be able to list all the activities of a device, within the time range of 60 seconds of a particular suspicious activity without writing any complicated queries.</p> <p>The solution should dynamically calculate the Risk score of a device based on 7-day rolling window of activity data. The Risk rating of remediated devices should change automatically as per rolling window period without any information from another solution.</p> <p>Solution should be able to use different sensors models in the same deployment without restrictions.</p>
24	Implementation and Operation	The bidder shall implement the solution according to the implementation document shared by the bidder and as approved by the procuring entity. The bidder shall conduct necessary pre and post deployment knowledge transfer session for the successful operation & administration of the solution in the future.
25	Support and Subscription	3 years with 24x7 support SLA



Sl. No. **69.**

Section VII – Purchaser’s Requirements

3.7 Detailed Technical Specifications and Requirements,

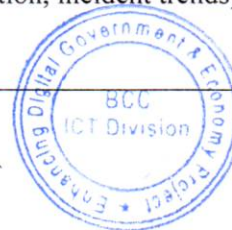
3.7.8 Ticketing, IT Service, IT Asset & NMS System

Page: 185

As Amended: for SL: 215-233 NMS Module B

Following Requirements added Page 185 of RFP Document:

Sl.	Feature	Requirement of Procuring Entity
215	Solution Type (NMS): Brand	To be mentioned by the bidder
216	Model	To be mentioned by the bidder
217	Country of Origin	To be mentioned by the bidder
218	Country of Manufacturer	To be mentioned by the bidder
219	Architecture and Scale	<ul style="list-style-type: none">- Must be Open Source and Community Supported- Must support monitoring of different devices/systems with both agent-based and agentless architecture- Must be scalable to support future growth- Must be able to collect metrics and logs to provide observability- Must support distributed and centralized monitoring options
220	Protocols Supported	<ul style="list-style-type: none">- SNMP, ICMP, TCP- NetFlow/sFlow/jFlow/IPFIX- Syslog- Agent based integrations
221	Monitoring Features	<ul style="list-style-type: none">- Real-time performance monitoring of different metrics (traffic, CPU, memory, disk utilization etc.)- Device/Host and link status monitoring- Service (e.g. Apache/Nginx/Tomcat etc.) Status Monitoring- Automatic host discovery- Topology visualization- Threshold-based alerting- Custom dashboards and reports creation feature
222	Visualization	<ul style="list-style-type: none">- Interactive Network Topology Map- Customizable Dashboards- Historical trend analysis with graphing capabilities
223	User Access and Security	<ul style="list-style-type: none">- Role-Based Access Control (RBAC)- Multi-user environment support- Secure web-based access- Audit logs for user activities
224	Integration	<ul style="list-style-type: none">- Integration with ITSM or Helpdesk platforms (open API support or other similar methods)- Built in native plugins or similar solution as well support for third-party plugins and extensions to extend the monitoring capabilities
225	Reporting	<ul style="list-style-type: none">- Automated reporting (availability, utilization, incident trends)- On-demand customizable reports- Export options: PDF, CSV, Excel



Sl.	Feature	Requirement of Procuring Entity
226	Alerts and Notifications	- Real-time alerts via Email, SMS, or API - Configurable alert thresholds
227	Delivery	On-premise Deployment in all CIIs
228	License Type	Open Source, Free to Use, Community-Supported. Optional commercial support to be proposed if available.
229	Training	On-site training for (BCC, NCSA & 2 Participants from each CII) at least 100 persons by experienced technical staff on the proposed platform.
230	Documentation	Complete user manuals, deployment guides, and troubleshooting guides to be provided
231	Support	Community Support must be available; optional 24/7 paid support package to be offered if applicable
232	Compliance	Must follow industry security best practices (encryption for data in transit, secure authentication mechanisms)
233	Support	Bidder shall provide 24/7 of 3 years service & support for offered solution



Sl. No. **70.**

Section VII – Purchaser’s Requirements

3.7 Detailed Technical Specifications and Requirements

Page: 185

As Amended: SL. 3.7.29 for VAPT Tools

Following Requirements added after 3.7.28 Malware Analysis Sandbox (On-premises) Page 224 of RFP Document:

3.7.29.1 Web Application Scanner

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5.	Architecture and Scale	<ul style="list-style-type: none">• Must be capable to support for scan for 12,000+ web vulnerabilities.• Must be capable to support scan for 7,000+ vulnerabilities in WordPress and WordPress plug-in.• Must support for multiple Users.• Must support for multiple Scan Engines.• Must support for continuous scanning.• Must support standard role-based access controls.• Must support to prepare compliance reports (HIPAA, PCI-DSS, ISO/IEC 27001, and more).• Must support to crawl HTML5 websites and AJAX-heavy clientside SPAs.• Must support for malware scanning/malware analyzer.• Must support for proof-based scanning technology (proof of exploit).• Must support for remediation advice.• Must support for technical support during license period.
6.	Delivery	On-premise
7.	License Count (Targets)	100
8.	License Period	1 year

3.7.29.2 API Scanner

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder

8

12



4.	Country of Manufacturer	To be mentioned by the bidder
5.	Protocol Support	Must have support for RESTful, SOAP, JMS, JDBC, and other services
6.	Functional Testing	Must have capability for Manual & Complex Scenario Testing for Soap, REST, HTTP, GraphQL, and more
		Must have capability for API Security testing: Boundary, Cross-Site, Fuzzing, SQL Injection, and more
		Must have capability for Advanced and Automated API Security Testing
		Must have capability for Coverage and Data-Driven API Testing
		Must have support for Endpoint Scanning
7.	Performance Testing	Must have support for Parallel Functional Testing/Load Testing
		Must have support for Virtual User Simulation with Load Profiles
8.	CI/CD Pipeline Integration	Must have support for Powerful Command-line Tools or Native Integrations with Jenkins, Git, etc.
9.	Support	Must have Product Support along with 24/7 Technical Support
10.	Delivery	On-premise
11.	License Qty.	01 (One)
12.	License Period	1 year
13.	License Type if applicable	Multiple users test on physical and virtual machine
14.	Edition if Applicable	API functional & security testing
15.	Training	Online local training by OEM instructor for 10 persons

3.7.29.3 The macOS and Linux Disassembler for Application Security Testing

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5.	Control Flow Graph	Must have Support to display a graphical representation of the control flow graph.
6.	Procedures	Must have Support to analyze function's prologues to extract procedural information such as basic blocks and local variables.
7.	Scriptable	Must have Support for features to invoked from Python scripts
8.	Debugger	Must have Support for LLDB or GDB to debug and analyze the binary in a dynamic way



8

NR

9.	Objective-C	Must have Support for retrieving Objective-C information in the files to analyze, like selectors, strings and messages sent.
10.	Decompiler	Must have Support for to present a pseudo-code representation of the procedures found in an executable.
11.	Delivery	On-premise
12.	License Qty.	01 (One)
13.	Software Updates	Product should receive 1 year software updates.
14.	License Type	Computer License

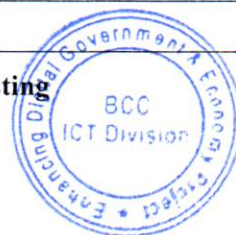
3.7.29.4 Laptop for Mobile Application Security Testing

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5.	Year of Manufacturer	Not before 2023
6.	Processor	Must have M3 Pro chip 11-core CPU with 5 performance cores and 6 efficiency cores Hardware-accelerated ray tracing 16-core Neural Engine
7.	Display	Must have 14.2-inch Liquid Retina XDR Display 3024x1964 1600 nits peak Brightness HDR Content 1 Billion Colors P3 Wide Color True Tone Technology 120Hz ProMotion Adaptive Refresh Rate
8.	Storage	Minimum 512GB SSD
9.	Memory	Minimum 18GB RAM
10.	Audio	Support for High Fidelity Six Speaker Force-Cancelling Woofers Wide Stereo Sound Dolby Atmos on Built-in Speakers High Impedance Headphones Supported
11.	Camera	1080p FaceTime HD camera
12.	Port Types	Must support for Three Thunderbolt 4 Ports 3.5mm Headphone Jack MagSafe 3 Port HDMI Port SDXC Card Slot
13.	Network	Support for Wi-Fi 6E (802.11ax) Bluetooth 5.3
14.	Graphics	Must support for 14-core GPU
15.	Power Source	Must have 72.4-Watt Hour Lithium-Polymer Battery 70W USB-C Power Adapter Fast-Charge Capability
16.	Converter	Mac Type – C, 8 in one hub
17.	Quantity	01(one)
18.	Warranty	(03) Three years full warranty

3.7.29.5 Mobile Device for Mobile Application Security Testing

8

✓



Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5.	Network Technology	GSM / HSPA / LTE
6.	Body Dimensions	Must be 143.6 x 70.9 x 7.7 mm (5.65 x 2.79 x 0.30 in)
7.	Weight	Must be 174 g (6.14 oz)
8.	SIM	Must support Nano-SIM
9.	Display	<input type="checkbox"/> Must have Super Retina OLED, HDR10, Dolby Vision, 625 nits (HBM) <ul style="list-style-type: none"> • Must have 5.8 inches, 84.4 cm² (~82.9% screen-to-body ratio) • Must have 1125 x 2436 pixels, 19.5:9 ratio (~458 ppi density)
10.	OS	Must be iOS 14.0 (version should not exceed 14.0)
11.	Chipset	Must have A11 Bionic (10 nm)
12.	CPU	Hexa-core 2.39 GHz (2x Monsoon + 4x Mistral)
13.	Storage	Minimum 64GB or more
14.	RAM	Minimum 3GB or more
15.	Main Camera	<ul style="list-style-type: none"> • Must have 12 MP, f/1.8, 28mm (wide), 1/3.0", 1.22µm, dual pixel PDAF, OIS • Must have 12 MP, f/2.4, 52mm (telephoto), 1/3.4", 1.0µm, PDAF, OIS, 2x optical zoom • Must support 4K@24/30/60fps, 1080p@30/60/120/240fps
16.	Selfie camera	<ul style="list-style-type: none"> • Must have 7 MP, f/2.2, 32mm (standard) • Must support SL 3D, (depth/biometrics sensor) • Must support 1080p@30fps, HDR
17.	WLAN	Must support Wi-Fi 802.11 a/b/g/n/ac, dual-band, hotspot
18.	Battery	<ul style="list-style-type: none"> • Must support Li-Ion 2716 mAh, non-removable (10.35 Wh) • Must support 15W wired, PD2.0
19.	Quantity	01 (One)
20.	Warranty	One (01) year full warranty



8

me

Sl. No. **71.**

Section VII – Purchaser’s Requirements

3.7 Detailed Technical Specifications and Requirements

As Amended: SL. 3.7.30 for Digital Forensic Tools

Following Requirements added after 3.7.29 VAPT Tools and Before SOC Training of RFP Document:

3.7.30.1 Password Breaking tool

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5	Features	<ul style="list-style-type: none">• Password recovery for 300+ file types-MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Bitcoin wallets, password managers, and many other applications.• Live memory analysis- Analyzes live memory images and hibernation files and extracts• encryption keys for hard disks, logins for Windows & Mac accounts, and passwords for files and websites, all in a single streamlined process.• Cross-platform Passware Kit Agents- Supports distributed password recovery with Agents for Windows, Linux, and Amazon EC2.• Passware Bootable Memory Imager- A UEFI compatible tool that acquires memory images of Windows, Linux, and Mac computers. Passware Memory Imager works with Windows <input type="checkbox"/> computers that have Secure Boot enabled.• Automatic updates- Includes automatic software updates with one year of Software• Maintenance and Support (SMS) subscription.• Hardware acceleration- Accelerated password recovery with multiple computers, NVIDIA and AMD GPUs, and Rainbow Tables.• Batch processing - Runs password recovery for groups of files and FDE images without user intervention.• Decryption of FDE- Decrypts or recovers passwords for APFS, Apple DMG, BitLocker, Dell, FileVault2, LUKS, McAfee, PGP, Symantec, and TrueCrypt/VeraCrypt disk images.• Encryption detection and analysis- Detects all encrypted files and hard disk images and reports the type of encryption and the complexity of the decryption.• Password Exchange- Password Exchange provides access to the list of passwords found by Passware Kit users worldwide, offering it as an advanced dictionary to improve chances of finding strong passwords.

Sl.	Feature	Requirement of Procuring Entity
		<ul style="list-style-type: none"> Email notifications- Automatically sends an email whenever a password is found or the recovery process gets finished. Mac T2 decryption add-on- Optional Passware Kit Forensic T2 Add-on recovers passwords for Macs equipped with Apple T2 Security Chip. Available for law enforcement and other types of government organizations. The Solutions Should Support for Windows 11 The Solutions Should Support for macOS Monterey The Solutions Should Password recovery for Acronis backups The Solutions Should have List of passwords supported by the Known Passwords attack The Solutions Should have LUKS2 decryption via memory
6.	Delivery	On-premise
7.	License Count (Dongle)	1
8.	License coverage	3 year (up to 30th June 2026)

3.7.30.2 Forensic Workstation

Sl.	Feature	Requirement of Procuring Entity
1.	Brand	To be mentioned by the bidder
2.	Model	To be mentioned by the bidder
3.	Country of Origin	To be mentioned by the bidder
4.	Country of Manufacturer	To be mentioned by the bidder
5.	Specification	<ul style="list-style-type: none"> Min. One (1) Intel Core i9 2.4 GHz (5.2GHz Turbo) Processor with 16-Cores & 24-Threads, Cache 30MB or higher Min.256 GB DDR4 ECC RAM 4800 MHz (8 x 16 GB) Min. One (1) 2 TB SSD for the Operating System set in Rapid Mode Min. One (1) Nvidia 4060 GeForce 16 GB GDDR6X Graphics Processing Unit Min. Two (2) 10TB HDD for Images / Data Min. One (1) 2.5" & 3.5" True Hot-Swap Bay Min. One (1) Four Port USB 3.0 Panel Min. One (1) Logicube Write Protect Bay – Custom Designed and supports IDE, SATA, SAS, USB, FireWire, and PCIe SSDs (M.2 SATA/ AHCI/ NVMe), PCIe and mini-PCIe cards with Optional Adapters Min. One (1) External Optical DVD-RW with 32X - SATA Form Factor USB 3.1 Gen. 2 USB Type A & C with Charging Ports, Min. 02(Two) 27"FHD IPS Anti-Glare Monitor Forensic Standard all items Windows 11 Pro license,



Sl.	Feature	Requirement of Procuring Entity
		<ul style="list-style-type: none"> Min. One (1) Advanced Cooling for the CPU Min. One (1) Windows 10 Professional 64-Bit Min. One (1) 1000W Power Supply Unit – Gold Rated
6.	Delivery	On-premise
7.	Quantity	3
8.	Warranty	Three (3) Years' full Warranty

3.7.30.3 Renewal of Existing Products

Sl. No.	Feature	Requirement of Procuring Entity
1.	Oxygen Forensic Detective -	Renewal of license for Oxygen Forensic Detective. License coverage up to Jun 2026. Quantity: 2 Pcs
2.	Detego Analyse Forensic. -	Renewal of license for Detego Analyse Forensic. License coverage up to Jun 2026. Quantity: 1 Pc
3.	Magnet AXIOM -	Renewal of license for Magnet AXIOM. License coverage up to Jun 2026. Quantity: 2 Pcs
4.	Belkasoft Evidence Center X -	Renewal of license for Belkasoft Evidence Center X. License coverage up to Jun 2026. Quantity: 1 Pc
5.	FTK Forensic Toolkit -	Renewal of license for FTK Forensic Toolkit. License coverage up to Jun 2026. Quantity: 1 Pc
6.	OpenText EnCase Forensic -	Renewal of license for OpenText EnCase Forensic. License coverage up to Jun 2026. Quantity: 1 Pc
7.	MD Next, Red and Cloud -	Renewal of license for MD Next, Red and Cloud. License coverage up to Jun 2026. Quantity: 1 Pc

3.7.30.4 Training

8

MZ



Sl. No.	Feature	Requirement of Procuring Entity
1	Training (for all the above items)	<p>1. At least Three-Level incremental certifications through min.15 (Fifteen) days training will be provided by the manufacturers for min. 04 (Four) officers for comprehensive hands-on training on all functionalities of Forensic Expert. The training must include Certification.</p> <p>2. The training must include hands-on practice on analyzing min.</p> <p>3. The training must include (but not be limited to) orientation, installation, configuration, operation, analysis & reporting all events as well as comprehensive use of all features/modules. Name and location of training venue shall be mentioned by the bidder.</p> <p>All trainings should be provided / arranged locally by authorized trainer of OEM.</p>
2	Standard User Manual	1 (one) set of operational manuals with delivery of product



8

me

Sl. No. 72.

Section VII-Purchasers' requirements

Page:234-237

As in Issued RFP:

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.

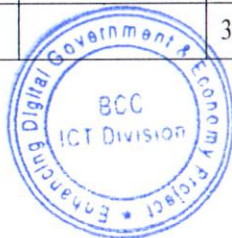
Line-Item No.	System / Item	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
0	Project Plan		N/A	ICT Tower	W3	-	W5	No
1	Security Information and Event Management (SIEM)		3.7.1	ICT Tower	W12	W16	W18	No
2	Security Orchestration, Automation, and Response (SOAR)		3.7.2	ICT Tower	W12	W16	W18	No
3	Privileged Access Management (PAM)		3.7.3	ICT Tower	W12	W16	W18	No
4	Endpoint Detection and Response (EDR)		3.7.4	ICT Tower	W12	W16	W18	No
5	Server Security		3.7.5	ICT Tower	W12	W16	W18	No



8

W2

Line-Item No.	System / Item	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
6	Next Generation Firewall for SOC (Qty. 02)		3.7.6	ICT Tower	W6	W8	W10	No
7	VPN Firewall for CII Integration (Qty. 02)		3.7.7	ICT Tower	W6	W8	W10	No
8	Ticketing, IT Service, IT Asset & NMS System		3.7.8	ICT Tower	W12	W16	W18	No
9	Network Behavior Analysis (NBA) with Sandboxing		3.7.9	ICT Tower	W12	W16	W18	No
10	Server Farm Switch (Qty. 04)		3.7.10	ICT Tower	W6	W8	W10	No
11	FC Switch (Qty. 02)		3.7.11	ICT Tower	W6	W8	W10	No
12	Perimeter Switch for CII Integration (Qty. 02)		3.7.12	ICT Tower	W6	W8	W10	No
13	Access Switch for SOC Room and Management (Qty. 02)		3.7.13	ICT Tower	W6	W8	W10	No
14	Virtualization Software		3.7.14	ICT Tower	W6	W8	W10	No
15	Physical Servers for On-Premise SOC Tools (Qty. 08)		3.7.15	ICT Tower	W6	W8	W10	No
16	Workstation (Qty. 15)		3.7.16	ICT Tower	W6	W8	W10	No
17	Laptop (Qty. 10)		3.7.17	ICT Tower	W6	W8	W10	No



Line-Item No.	System / Item	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
18	FC Storage (Qty. 01)		3.7.18	ICT Tower	W6	W8	W10	No
19	42U Server Rack		3.7.19	ICT Tower	W6	W8	W10	No
20	SOC Room		3.7.20	ICT Tower	W6	W8	W10	No
21	Digital Boards (86" IFP or Equivalent)		3.7.21	ICT Tower	W6	W8	W10	No
22	Video Wall System (4x55" with HDMI Matrix and Accessories)		3.7.22	ICT Tower	W6	W8	W10	No
23	20 KVA Online UPS (Qty. 01)		3.7.23	ICT Tower	W6	W8	W10	No
24	Face & Fingerprint Time Attendance Access Control System		3.7.24	ICT Tower	W6	W8	W10	No
25	Solutions Trainings (On-Site)		3.7.25	ICT Tower	W6	W8	W10	No
26	Deployment and Knowledge Transfer Training (On-Site)		3.7.26	ICT Tower	W6	W8	W10	No
27	External Attack Surface Management		3.7.27	ICT Tower	W12	W16	W18	No
28	Malware Analysis Sandbox (On-Premise)		3.7.28	ICT Tower	W6	W8	W10	No



8

N2

Line-Item No.	System / Item	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
29	SOC Trainings (With Certification Exams)		3.7.29	ICT Tower	W4	-	W18	No
30	SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)		3.7.30	ICT Tower	W4	-	W18	No
31	Installation & Implementation of NSOC System		3.7.31	ICT Tower	-	W7	W19	No
32	Project Management for SOC System Implementation		3.7.32	ICT Tower	-	-	W19	No
33	Operational Acceptance of the System		N/A	ICT Tower	-	-	W20	Yes

nr

8



As Amended:

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.

Line-Item No.	System / Item	Subsystem / Item	Configuration Table No.	Site / Site Code	Delivery (weeks from Effective Date)	Installation (weeks from Effective Date)	Acceptance (weeks from Effective Date)	Liquidated Damages Milestone
0	Project Plan		N/A	ICT Tower	W3	-	W5	No
1	Security Information and Event Management (SIEM)		3.7.1	ICT Tower	W12	W16	W18	No
2	Security Orchestration, Automation, and Response (SOAR)		3.7.2	ICT Tower	W12	W16	W18	No
3	Privileged Access Management (PAM)		3.7.3	ICT Tower	W12	W16	W18	No
4	Endpoint Detection and Response (EDR)		3.7.4	ICT Tower	W12	W16	W18	No
5	Server Security		3.7.5	ICT Tower	W12	W16	W18	No
6	Next Generation Firewall for SOC (Qty. 02)		3.7.6	ICT Tower	W6	W8	W10	No



8

22

7	VPN Firewall for CII Integration (Qty. 02)		3.7.7	ICT Tower	W6	W8	W10	No
8	Ticketing, IT Service, IT Asset & NMS System		3.7.8	ICT Tower	W12	W16	W18	No
9	Network Behavior Analysis (NBA) with Sandboxing		3.7.9	ICT Tower	W12	W16	W18	No
10	Server Farm Switch (Qty. 04)		3.7.10	ICT Tower	W6	W8	W10	No
11	FC Switch (Qty. 02)		3.7.11	ICT Tower	W6	W8	W10	No
12	Perimeter Switch for CII Integration (Qty. 02)		3.7.12	ICT Tower	W6	W8	W10	No
13	Access Switch for SOC Room and Management (Qty. 02)		3.7.13	ICT Tower	W6	W8	W10	No
14	Virtualization Software		3.7.14	ICT Tower	W6	W8	W10	No
15	Physical Servers for On-Premise SOC Tools (Qty. 08)		3.7.15	ICT Tower	W6	W8	W10	No
16	Workstation (Qty. 15)		3.7.16	ICT Tower	W6	W8	W10	No

8

me



17	Laptop (Qty. 10)		3.7.17	ICT Tower	W6	W8	W10	No
18	FC Storage (Qty. 01)		3.7.18	ICT Tower	W6	W8	W10	No
19	42U Server Rack		3.7.19	ICT Tower	W6	W8	W10	No
20	SOC Room		3.7.20	ICT Tower	W6	W8	W10	No
21	Digital Boards (86" IFP or Equivalent)		3.7.21	ICT Tower	W6	W8	W10	No
22	Video Wall System (4x55" with HDMI Matrix and Accessories)		3.7.22	ICT Tower	W6	W8	W10	No
23	20 KVA Online UPS (Qty. 01)		3.7.23	ICT Tower	W6	W8	W10	No
24	Face & Fingerprint Time Attendance Access Control System		3.7.24	ICT Tower	W6	W8	W10	No
25	Solutions Trainings (On-Site)		3.7.25	ICT Tower	W6	W8	W10	No
26	Deployment and Knowledge Transfer Training (On-Site)		3.7.26	ICT Tower	W6	W8	W10	No



8

27	External Attack Surface Management		3.7.27	ICT Tower	W12	W16	W18	No
28	Malware Analysis Sandbox (On-Premise)		3.7.28	ICT Tower	W6	W8	W10	No
29	VAPT Tools		3.7.29	ICT Tower	W6	W8	W10	No
30	Digital Forensic Tools		3.7.30	ICT Tower	W6	W8	W10	No
31	SOC Trainings (With Certification Exams)		3.7.31	ICT Tower	W4	-	W18	No
32	SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)		3.7.32	ICT Tower	W4	-	W18	No
33	Installation & Implementation of NSOC System		3.7.33	ICT Tower	-	W7	W19	No
34	Project Management for SOC System Implementation		3.7.34	ICT Tower	-	-	W19	No
35	Operational Acceptance of the System		N/A	ICT Tower	-	-	W20	Yes

8

~2



Sl. No. 73.

Section VII-Purchasers' requirements

Page:241-244

As in Issued RFP:

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS):

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1	Security Information and Event Management (SIEM)	3.7.1	ICT Tower	1 Unit
2	Security Orchestration, Automation, and Response (SOAR)	3.7.2	ICT Tower	1 Unit
3	Privileged Access Management (PAM)	3.7.3	ICT Tower	1 Unit
4	Endpoint Detection and Response (EDR)	3.7.4	ICT Tower	1 Unit
5	Server Security	3.7.5	ICT Tower	1 Unit
6	Next Generation Firewall for SOC	3.7.6	ICT Tower	2 Unit
7	VPN Firewall for CII Integration	3.7.7	ICT Tower	2 Unit
8	Ticketing, IT Service, IT Asset & NMS System	3.7.8	ICT Tower	1 Unit



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
9	Network Behavior Analysis (NBA) with Sandboxing	3.7.9	ICT Tower	1 Unit
10	Server Farm Switch	3.7.10	ICT Tower	2 Unit
11	FC Switch	3.7.11	ICT Tower	2 Unit
12	Perimeter Switch for CII Integration	3.7.12	ICT Tower	2 Unit
13	Access Switch for SOC Room and Management	3.7.13	ICT Tower	2 Unit
14	Virtualization Software	3.7.14	ICT Tower	1 Unit
15	Physical Servers for On-Premise SOC Tools	3.7.15	ICT Tower	8 Unit
16	Workstation	3.7.16	ICT Tower	15 Unit
17	Laptop	3.7.17	ICT Tower	10 Unit
18	FC Storage	3.7.18	ICT Tower	1 Unit
19	42U Server Rack	3.7.19	ICT Tower	2 Unit
20	SOC Room	3.7.20	ICT Tower	1 Unit
21	Digital Boards (86" IFP or Equivalent)	3.7.21	ICT Tower	1 Unit
22	Video Wall System (4x55" with HDMI Matrix and Accessories)	3.7.22	ICT Tower	1 Unit

8 12



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
23	20 KVA Online UPS	3.7.23	ICT Tower	1 Unit
24	Face & Fingerprint Time Attendance Access Control System	3.7.24	ICT Tower	1 Unit
25	Solutions Trainings (On-Site)	3.7.25	ICT Tower	Lot
26	Deployment and Knowledge Transfer Training (On-Site)	3.7.26	ICT Tower	Lot
27	External Attack Surface Management	3.7.27	ICT Tower	1 Unit
28	Malware Analysis Sandbox (On-Premise)	3.7.28	ICT Tower	1 Unit
29	SOC Trainings (With Certification Exams)	3.7.29	ICT Tower	Lot
30	SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)	3.7.30	ICT Tower	Lot
31	Installation & Implementation of NSOC System	3.7.31	ICT Tower	Lot
32	Project Management Oversight (Non-Priced) for NSOC System Implementation	3.7.32	ICT Tower	Lot



Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
33	Warranty including Maintenance of IT/Non-IT Hardware, Software and Related Services of NSOC	-	ICT Tower	Three (3) for Years from the date of Operational Acceptance

Note: Component No: '33', Relevant Technical Specifications No. '3.7.32', "Project Management Oversight (Non-Priced) for NSOC System Implementation" The cost of this service shall be considered embedded in each technical line item and shall not be priced separately.

8

12



As Amended:

SYSTEM INVENTORY TABLE (SUPPLY AND INSTALLATION COST ITEMS)

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
1	Security Information and Event Management (SIEM)	3.7.1	ICT Tower	1 Unit
2	Security Orchestration, Automation, and Response (SOAR)	3.7.2	ICT Tower	1 Unit
3	Privileged Access Management (PAM)	3.7.3	ICT Tower	1 Unit
4	Endpoint Detection and Response (EDR)	3.7.4	ICT Tower	1 Unit
5	Server Security	3.7.5	ICT Tower	1 Unit
6	Next Generation Firewall for SOC	3.7.6	ICT Tower	2 Unit
7	VPN Firewall for CII Integration	3.7.7	ICT Tower	2 Unit
8	Ticketing, IT Service, IT Asset & NMS System	3.7.8	ICT Tower	1 Unit
9	Network Behavior Analysis (NBA) with Sandboxing	3.7.9	ICT Tower	1 Unit
10	Server Farm Switch	3.7.10	ICT Tower	2 Unit
11	FC Switch	3.7.11	ICT Tower	2 Unit
12	Perimeter Switch for CII Integration	3.7.12	ICT Tower	2 Unit
13	Access Switch for SOC Room and Management	3.7.13	ICT Tower	2 Unit
14	Virtualization Software	3.7.14	ICT Tower	1 Unit
15	Physical Servers for On-Premise SOC Tools	3.7.15	ICT Tower	8 Unit



8

22

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
16	Workstation	3.7.16	ICT Tower	15 Unit
17	Laptop	3.7.17	ICT Tower	10 Unit
18	FC Storage	3.7.18	ICT Tower	1 Unit
19	42U Server Rack	3.7.19	ICT Tower	2 Unit
20	SOC Room	3.7.20	ICT Tower	1 Unit
21	Digital Boards (86" IFP or Equivalent)	3.7.21	ICT Tower	1 Unit
22	Video Wall System (4x55" with HDMI Matrix and Accessories)	3.7.22	ICT Tower	1 Unit
23	20 KVA Online UPS	3.7.23	ICT Tower	1 Unit
24	Face & Fingerprint Time Attendance Access Control System	3.7.24	ICT Tower	1 Unit
25	Solutions Trainings (On-Site)	3.7.25	ICT Tower	Lot
26	Deployment and Knowledge Transfer Training (On-Site)	3.7.26	ICT Tower	Lot
27	External Attack Surface Management	3.7.27	ICT Tower	1 Unit
28	Malware Analysis Sandbox (On-Premise)	3.7.28	ICT Tower	1 Unit
29	VAPT Tools	3.7.29	ICT Tower	Lot
30	Digital Forensic Tools	3.7.30	ICT Tower	Lot
31	SOC Trainings (With Certification Exams)	3.7.31	ICT Tower	Lot



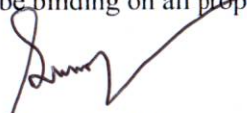
8

2

Component No.	Component	Relevant Technical Specifications No.	Additional Site Information (e.g., building, floor, department, etc.)	Quantity
32	SOC Trainings (With Certification Exams, On-Site Global Training Partner Premises) (Free of Cost)	3.7.32	ICT Tower	Lot
33	Installation & Implementation of NSOC System	3.7.33	ICT Tower	Lot
34	Project Management Oversight (Non-Priced) for NSOC System Implementation	3.7.34	ICT Tower	Lot
35	Warranty including Maintenance of IT/Non-IT Hardware, Software and Related Services of NSOC	3.7.35	ICT Tower	Three (3) for Years from the date of Operational Acceptance

Note: Component No: '34', Relevant Technical Specifications No. '3.7.34', "Project Management Oversight (Non-Priced) for NSOC System Implementation" The cost of this service shall be considered embedded in each technical line item and shall not be priced separately.

All other terms and conditions of RFP No: EDGE-G20 shall remain unchanged. This Addendum No. 1 shall be considered **an integral part** of the RFP document and shall be binding on all proposers who have obtained the RFP document from the Purchaser in accordance with ITP 6.3.


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

